UNIK
UNIVERSITY GRADUATE CENTER

Human Factors in IT Security

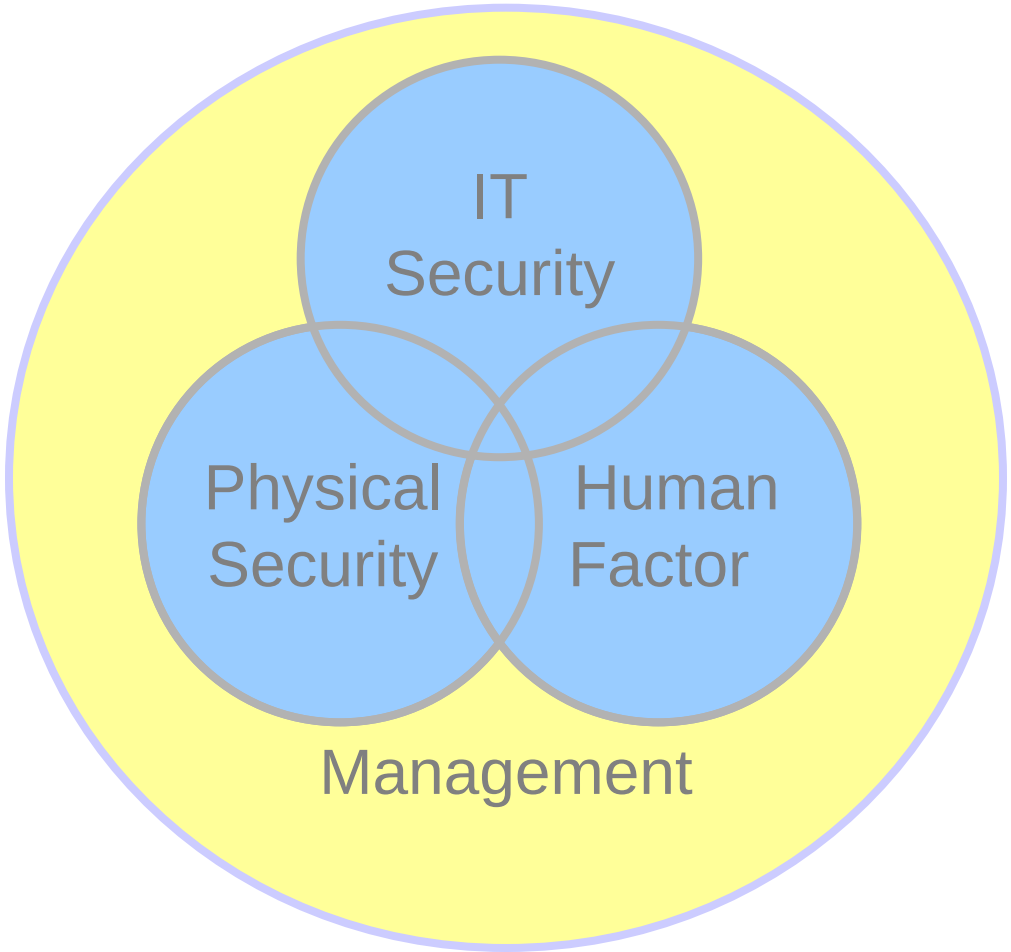
NISNet Winter School

Finse, April 2010

Audun Jøsang, UiO/UNIK – QUT

http://persons.unik.no/josang/

Components of Security



The Human Factor

- Personnel integrity
  - Making sure personnel do not become attackers
- People as defence
  - Making sure personnel do not fall victim to social engineering attacks
- Security Usability
  - Making sure people can operate security systems correctly

Personnel Integrity

Preventing employees from becoming attackers

- Consider:
  - Employees
  - Executives
  - Customers
  - Visitors
  - Contractors & Consultants
- All these groups obtain some form of access privileges
- How to make sure privileges are not abused?

Personnel crime statistics

- Organisations report that large proportion of computer crimes originate from inside
- US Statistics (CSI/FBI) 2005
  - http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf
  - 71% had inside (65% had external) computer crime attacks
- Australian Statistics (AusCERT) 2006
  - http://www.auscert.org.au/images/ACCSS2006.pdf
  - 30% had inside (82% had external) electronic attacks

Personnel Integrity

- A company's existence depends on the integrity of its employees.
- New employees may get access to extremely sensitive and confidential information.
- The new employee's ethical outlook is *a priori* unknown.
- Unauthorized release of sensitive information could destroy reputation or cause financial damage
- An employee, who has just accepted a position with a major competitor, may want to steal important trade secrets.

Hiring Practices

- Employers are often reluctant to release information about former staff.
- Former employees have successfully sued corporations and supervisors for making derogatory statements to prospective employers.
- Consider:
  - Informal phone calls
  - Ask for reference authorization and consider “hold-harmless agreement” for written requests

Hiring Practices

- Reference authorization and hold-harmless agreement
  - The applicant authorises the disclosure of past employment information and releases both the prospective employer and the former employer from all claims and liabilities arising from the release of such information.
  - Should have: signature of applicant, releases former & prospective employers, and clearly specifies the type of information that may be divulged.

Personnel Departure

- Different reasons for departure
  - Voluntary
  - Redundancy
  - Termination
- Different types of actions
  - Former employee may keep some privileges
  - Revoke all privileges
  - Escort to the exit.
- During exit interview, terms of original employment agreement reviewed (i.e. non-compete, wrongful disclosure, etc.

People as Defence

People as Defence:
Protecting against social engineering attacks

- Social Engineering Basics
  - "Management of human beings according to their place and function in society" (Websters Dictionary)
  - Everybody practices social engineering
    - Social interactions, negotiations, diplomacy
  - Social engineering can also be used as part of attacking information systems

Social Engineering Attacks

- According to Kevin Mitnick:
  - “The biggest threat to the security of a company is not a computer virus, an unpatched hole in a program, or a badly installed firewall. In fact the biggest threat could be you.”
  - “What I found personally to be true was that it’s easier to manipulate people rather than technology. Most of the time, organisations overlook that human element”.

From “How to hack people”, BBC NewsOnline, 14 Oct 2002

“Social engineering is the practice of obtaining confidential information by manipulation of legitimate users” *Wikipedia*

- *Social engineering attacks are powerful because users are the weakest link in security.”*

The issue:

The underlying principle behind social engineering is that it can be easier to trick people than to hack into computing systems by force. Social engineers get personal information or access to computing systems by exploiting people’s natural tendency to want to trust and be helpful, and by taking advantage of our tendency to act quickly when faced with a crisis.

A Social Engineer will commonly use e-mail, the internet, or the telephone to trick people into revealing sensitive information or get them to do something that is against policy.

Some typical ways of practicing of social engineering attacks are:

- ***Spam scams/phishing:*** *deceptive e-mails designed to compromise computers, steal personal or private information or passwords*
- ***Impersonation:*** *attackers pose as someone in authority, or an IT representative, in order to obtain information or direct access to systems.*
- ***Dumpster diving:*** *the practice of going through trash to obtain valuable information, often as a first stage to subsequent attacks*

Spear Phishing

- Phishing that targets a specific group
- Cleverly designed deceit
- Often based in intimate knowledge of the victim
- Can be extremely hard to detect
- From a statistical viewpoint, you will fall victim to spear phishing if hit a sufficient number of times

Climate Spear Phishing

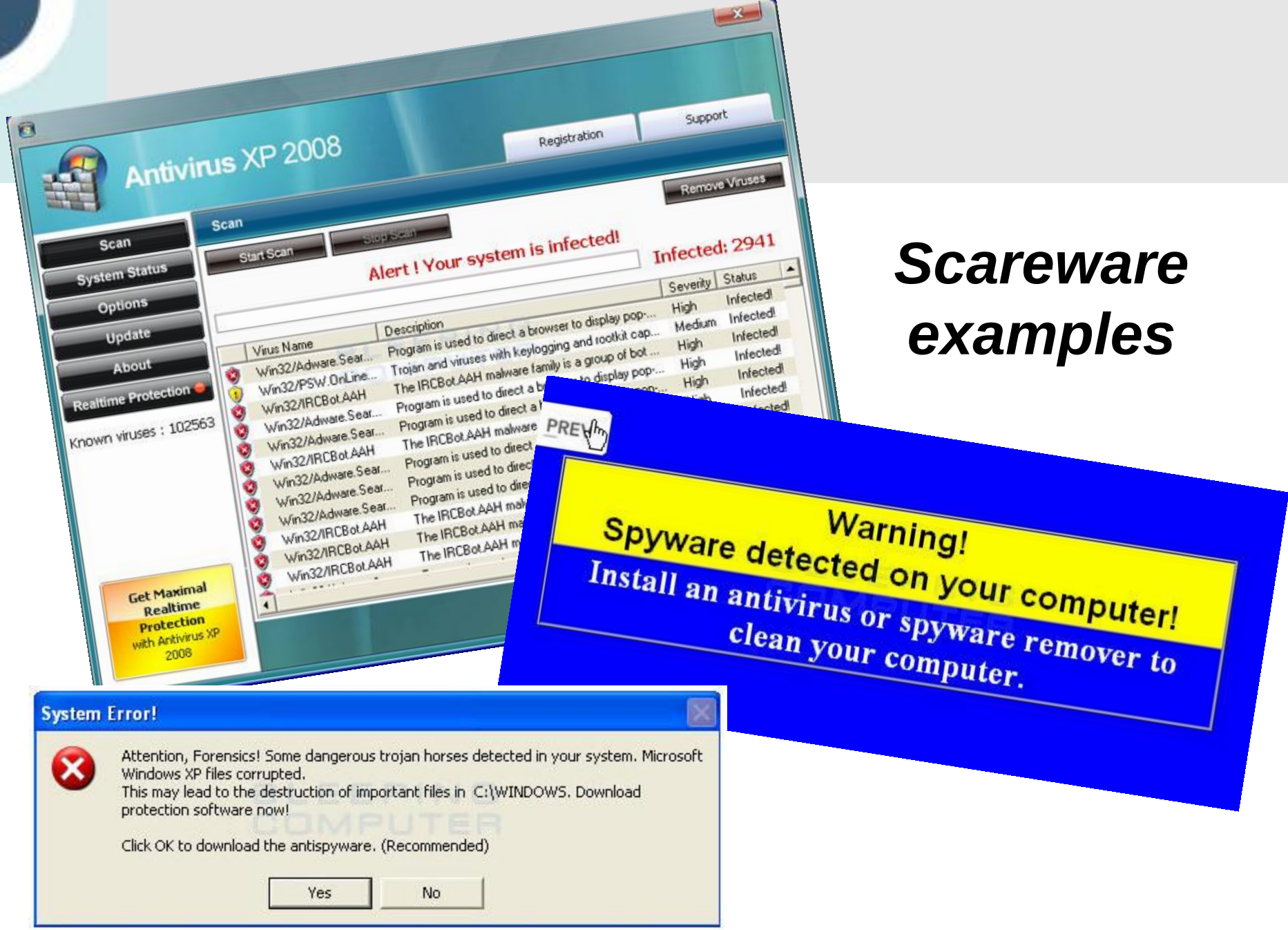
- In February 2010 hackers sent e-mails to several companies in Europe, Japan and New Zealand which appeared to originate from the Potsdam-based German Emissions Trading Authority (DEHSt)
- The e-mail said that the recipient needed to re-register on the agency's Web site to counter the threat of hacker attacks, but it instead pointed to a fake site which stole the credentials
- The hackers fraudulently obtained European greenhouse gas emissions allowances and resold them for millions of dollars.
- The scam forced DEHSt to stop the trading of emission allowances.

Scareware

- Pop-ups that appear to provide useful advice
- In reality, it is an attempt to trick the user to install software
- The software will get full access to the system
- Total system compromise

- Can be extremely hard to detect when cleverly designed

Scareware examples



UNIK

SE Tactics: Develop Trust

- People are naturally helpful and trusting
- Ask during seemingly innocent conversations
- Slowly ask for increasingly important information
- Learn company lingo, names of key personnel, names of servers and applications
- Cause a problem and subsequently offer your help to fix it (aka. reverse social engineering, see later)
- Talk negatively about common enemy
- Talk positively about common hero

SE Tactics: Induce strong affect

- Heightened emotional state makes victim
  - Less alert
  - Less likely to analyse deceptive arguments
- Triggered by attacker by creating
  - Excitement (“you have won a price”)
  - Fear (“you will loose your job”)
  - Confusion (contradictory statements)

SE Tactics: Overload

- Reduced the target's ability to scrutinize arguments proposed by the attacker
- Triggered by
  - Providing large amounts of information to produce sensory overload
  - Providing arguments from an unexpected angle, which forces the victim to analyse the situation from new perspective, which requires additional mental processing

SE Tactics: Reciprocation

- Exploits our tendency to return a favour
  - Even if the first favour was not requested
  - Even if the return favour is more valuable
- Double disagreement
  - If the attacker creates a double disagreement, and gives in on one, the victim will have a tendency to give in on the other
- Expectation
  - If the victim is requested to give the first favour, he will believe that the attacker becomes a future ally

SE Tactics: Diffusion of Responsibility and Moral Duty

- Make the target feel the he or she will not be held responsible for actions
- Make the target feel that satisfying attacker's request is a moral duty
- Convince the target that it's common to breach the security policy
  - "... everybody does it"
- Make the target believe that the policy has already been breached, so doing it again doesn't change anything
  - "... you gave the password to your other colleague, so why not to me"

SE Tactics: Authority

- People are conditioned to obey authority
  - Milgram and other experiments
  - Considered rude to even challenge the veracity of authority claim
- Triggered by
  - Faking credentials
  - Faking to be a director or superior
  - Skilful acting (con artist)

SE Tactics: Commitment Creep

- People have a tendency to follow commitments, even when recognising that it might be unwise.
- It's often a matter of showing personal consistency and integrity
- Triggered e.g. by creating a situation where one commitment naturally or logically follows another.
  - First request is harmless
  - Second request causes the damage

SE Tactics:
Reverse Social Engineering

- This is when the hacker creates a persona that appears to be in a position of authority so that employees will ask him for information, rather than the other way around.
- If researched, planned and executed well, reverse social engineering attacks may offer the hacker an even better chance of obtaining valuable data from the employees however, this requires a great deal of preparation, research, and pre-hacking to pull off.

SE Tactics:
Reverse social engineering (cont.)

- The three parts of reverse social engineering attacks are sabotage, advertising, and assisting.

1. The hacker *sabotages* a network, causing a problem arise.
2. That hacker then *advertises* that he is the appropriate contact to fix the problem,
3. and then, when he comes to *fix* the network problem, he requests certain bits of information from the employees and gets what he really came for.

- They never know it was a hacker, because their network problem goes away and everyone is happy.

Multi-Level Defence against Social Engineering Attacks

Source: David Gragg:
http://www.sans.org/rr/whitepapers/engineering/

SE Defence: Foundation

- Security policy to address SE attacks
  - The policy will always be the foundation of information security
  - Should address practices related to
    - Access controls
    - Account set-up
    - Password changes
    - Shredding
    - Visitor escorting
    - Authority obedience
  - Policy must not define practices that a SE attacker would use.

SE Defence: Awareness

- Security awareness training for all staff
  - Understanding SE tactics
  - Learn to recognise SE attacks
  - Know when to say “no”
  - Know what is sensitive
  - Understand their responsibility
  - Understand the danger of casual conversation
  - Friends are not always friends
  - Passwords are personal
  - Uniforms are cheap
- Awareness of policy shall make personnel feel that the only choice is to resist SE attempts

SE Defence: Fortress

- Resistance training for key personnel
  - Consider: Reception, Help desk, Sys.Admin., Customer service,
- Fortress training techniques
  - Inoculation
    - Expose to SE arguments, and learn counterarguments
  - Forewarming
    - of content and intent
  - Reality check:
    - Realising own vulnerability,

SE Defence: Persistence

- Ongoing reminders
  - SE resistance will quickly diminish after a training session
  - Repeated training
  - Reminding staff of SE dangers
    - Posters
    - Messages
    - Tests

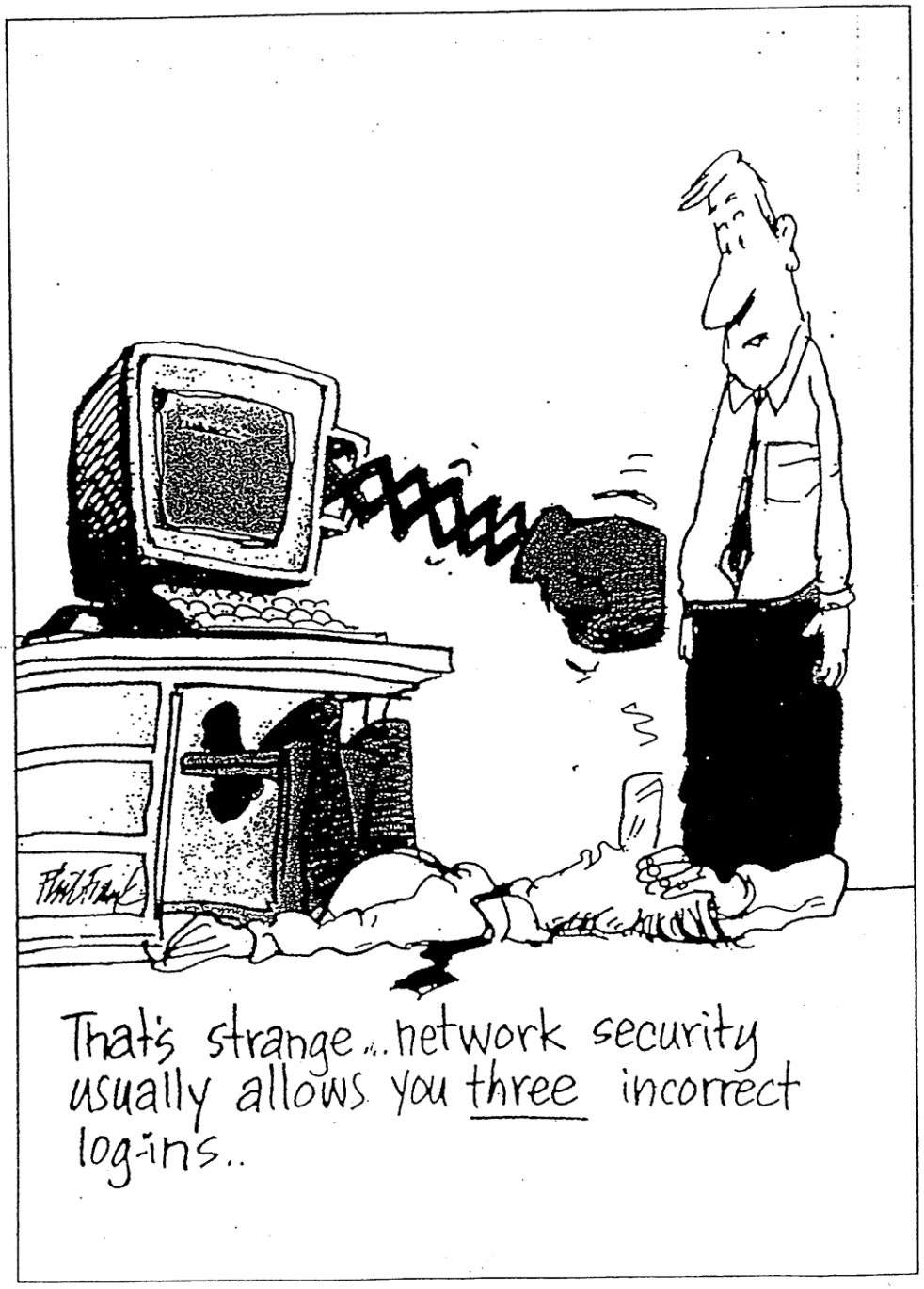
SE Defence: Gotcha

- Social Engineering Detectors
  - Filters and traps designed to expose SE attackers
- Consider:
  - The justified Know-it-all
    - Person who knows everybody
  - Centralised log of suspicious events
    - Can help discover SE patterns
  - Call backs mandatory by policy
  - Key questions, e.g. personal details
  - “Please hold” mandatory by policy
    - Time to think and log event
  - Deception
    - Bogus question
    - Login + password of “alarm account” on yellow sticker

SE Defence: Offensive

- Incident response
  - Well defined process for reporting and reacting to
    - Possible SE attack events,
    - Cases of successful SE attacks
- Reaction should be vigilant and aggressive
  - Go after SE attacker
  - Proactively warn other potential victims

Security Usability



Kerckhoffs 1883

- Auguste Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires,* IX(38):5-38 (January), and 161-191 (February), 1883.
- Famous principle; *"security by obscurity should be avoided"*
- Also defined security usability principles

Auguste Kerckhoffs

Kerckhoffs' security principles

1. The system must be substantially, if not mathematically, undecipherable;
2. The system must not require secrecy and can be stolen by the enemy without causing trouble;
3. It must be easy to communicate and remember the keys without requiring written notes, it must also be easy to change or modify the keys with different participants;
4. The system ought to be compatible with telegraph communication;
5. The system must be portable, and its use must not require more than one person;
6. Finally, regarding the circumstances in which such a system is applied, it must be easy to use and must neither require stress of mind nor the knowledge of a long series of rules.

Saltzer and Schroeder 1975

- Jerome H. Saltzer and Michael D. Schroeder. The Protection of Information in Computer Systems". *Communications of the ACM 17, 7 (July 1974).* 1975

Jerome Saltzer

- *It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.*
- *To the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized.*
- *If the user must translate his image of his protection needs into a radically different specification language, he will make errors.*

Michael Schroeder

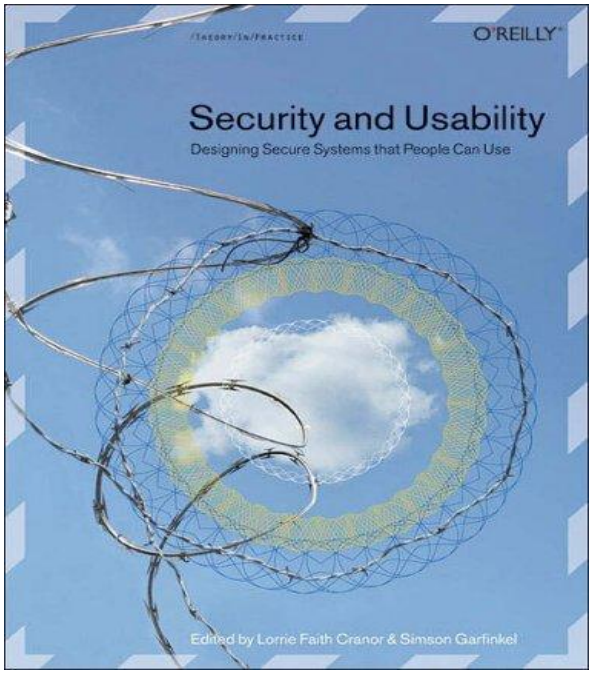
A collection of articles on security usability

Security and Usability: Designing secure system that people can use.

Lorrie Faith Cranor

Simpson Garfinkel.

(editors) 2005.



Adams & Sasse - 1999

- Anne Adams & Martina Angela Sasse (1999): **Users Are Not The Enemy: Why users compromise security mechanisms and how to take remedial measures.** Communications of the ACM
- Many users' knowledge about security is inadequate
- Users will shortcut security mechanisms that get in the way of their goals/tasks
- Security policies often make impossible demands of users
- Users lose respect for security, downward spiral in behaviour
-

Anne Adams

Angela Sasse

Whitten & Tygar 1999

- Alma Whitten and J.D. Tygar.
- ***Why Johnny Can't Encrypt: A Usability Evaluation of PGP5.0.***

  In *Proceedings of the 8th USENIX Security Symposium,* Washington, D.C. 1999.

Alma Whitten

Doug Tygar

Why Johnny Can't Encrypt. A Usability Evaluation of PGP 5.0

- PGP 5.0 had good usability from a traditional CHI (Computer-Human Interface) perspective.
- Still, 8 out of 12 participants were unable to encrypt and sign a message within 90min.
- Usability problems identified:
  - Misunderstood metaphors
  - No direct utility by security
  - Policy abstraction
  - Lack of feedback
  - The open barn door
  - Finding the weakest link

Whitten and Tygar's usability principles

- Effective security requires a different usability standard.
- Users must:
  - be reliably made aware of the security tasks they need to perform
  - be able to figure out how to successfully perform those tasks
  - not make dangerous errors
  - be sufficiently comfortable with the interface to continue using it

Jøsang, Alfayyadh, Grandison, Alzomai, McNamara 2007

- A. Jøsang, B. AlFayyadh, T. Grandison, M. Alzomai and J. McNamara. **Security Usability Principles for Vulnerability Analysis and Risk Assessment.** *Proceedings ACSAC 2007*

- *"Poor security usability represents a vulnerability. Must be included in standard vulnerability and risk analysis.*

- Security usability vulnerability analysis principles

Security usability vulnerabilities
Jøsang et al.

Security usability vulnerabilities exist when:

1. *Users don't know or understand what conclusion is required for making an informed security decision.*
2. *Systems do not provide the user with sufficient information for deriving a security conclusion.*
3. *An intolerable mental or manual load is required for deriving a security conclusion.*
4. *An intolerable mental or manual load is required for deriving security conclusions for any practical number of instances.*

Implications of Current Landscape

- Security systems must be viewed as socio-technical systems that depend on the social context in which they are embedded to function correctly.
- There is a very real difference between the degree by which systems can be considered theoretically secure (assuming they are correctly operated) and actually secure (acknowledging that often they will be operated incorrectly).

Difference between poor usability and poor security usability

- Usage
  - Poor usability in an IT system prevents people from using it
  - Poor security usability still allows people to use the system, but in an insecure way.
- Feedback
  - When you do something wrong in an IT application you normally notice because of the feedback you get
  - When you do something wrong in a security application you don’t notice because you get no feedback

Towards usable security (Whitten, 2004)

"… the usability problem for security is difficult to solve precisely because security presents qualitatively different types of usability challenges from those of other types of software […] making security usable will require the creation of user interface design methods that address those challenges."

Security / Usability Trade-off

- In many cases, there appears to be a trade-off between usability and theoretical security.
- It may be meaningful to reduce the level of theoretical security to improve the overall level of actual security.
- E.g.
  - User-friendly passwords
  - Remote villages and ATMs
- Policy should state the acceptable reduction in security for a specific security aspect
  - Implicitly in order to improve the overall security

Security Learning

- Good metaphors are important for learning
- Many security concepts do not have intuitive metaphors
- Better avoid metaphors than use bad ones
- Define new security concepts
  - and give them semantic content
- Security learning design
  - Design systems to facilitate good security learning
  - Largely unexplored field

Metaphors and mental models

- Users must have the correct mental model
- Metaphors can be practical, but
  - Must provide the right mental model
  - Wrong mental model can be a source of error

- Good metaphors:
  - Cryptographic key, access control
- Bad metaphors:
  - Firewall, trusted computing

More bad security metaphors

- Metaphors used by security experts as shorthand for communicating with each other do not work for wider audience
  - “key” cues the wrong mental model – not like locks and keys for physical access control
  - Meaning of “public” and “private” is different from everyday language
  - Not clear why a “digitally signed” message = “hasn’t been tampered with” – most users think it means it is from who it says it is …

From security learning pessimism... ... to security learning optimism

"… when presented with a software programme incorporating visible public key cryptography, users often complained during the first 10-15 minutes of the testing that they would expect 'that sort of thing' *to be handled invisibly. As their exposure to the software continued and their understanding of the security mechanism grew, they generally ceased to make that complaint."*

Alma Whitten's thesis, 2004

The power of security learning

"There are significant benefits to supporting users in developing a certain base level in generalizable security knowledge. A user who knows that, regardless of what application is in use, one kind of tool protects the privacy of transmission, a second kind protects the integrity of transmission, and a third kind protects the access to local resources, is much more empowered than one who must start afresh with each application."

Alma Whitten's thesis, 2004

How much security learning?

The next slide represents the view on security learning expressed by Eric Norman (University of Wisconsin) posted to the Yahoo HCISec mailing group, cited by Sasse in talk at PKI R&D workshop 2006

Yahoo HCISec post – part 1

"Those of us who grew up on the north side of Indianapolis have this thing for top 10 lists. At least one of us (me) believes the following: when it comes to PKI and security, users are going to have to learn something. I'm not sure just what that something is; I know it's not the mathematics of the RSA algorithm, but I believe that no matter what, there's something that they are just going to have to learn. It's like being able to drive down the concrete highway safely."

Yahoo HCISec post – part 2

"You don't have to learn about spark plugs and distributors, but you do have to learn how to drive, something about what the signs mean, what lines painted on the road mean, and so forth. Nobody can do this for you; each user (driver) is going to have to learn it for themselves. In order to get a better handle on just what it is that folks are going to have to learn, I'm trying to come up with a top 10 list of things that must be learned. Here's what I have so far with some help from some other folks I know who are more technophiles than human factors people. There are two lists: one for users and the other for administrators, developers, etc."

Yahoo HCISec post – part 3
Things PKI users to have to learn

1. How to import a trust anchor.
2. How to import a certificate.
3. How to protect your privates (private keys, that is).
4. How to apply for a certificate in your environment.
5. Why you shouldn't ignore PKI warnings.
6. How to interpret PKI error messages.
7. How to turn on digital signing.
8. How to install someone's public key in your address book.
9. How to get someone's public key.
10. How to export a certificate.

Yahoo HCISec post – part 4
… and

11. Risks of changing encryption keys.
12. How to interpret security icons in sundry browsers.
13. How to turn on encryption.
14. The difference between digital signatures and .signature files.
15. What happens if a key is revoked.
16. What does the little padlock *really* mean.
17. What does it mean to check the three boxes in Netscape/Mozilla?
18. What does "untrusted CA' mean in Netscape/Mozilla?
19. How to move and install certificates and private keys.

Yahoo HCISec post – part 5
Developers, administrators, etc.

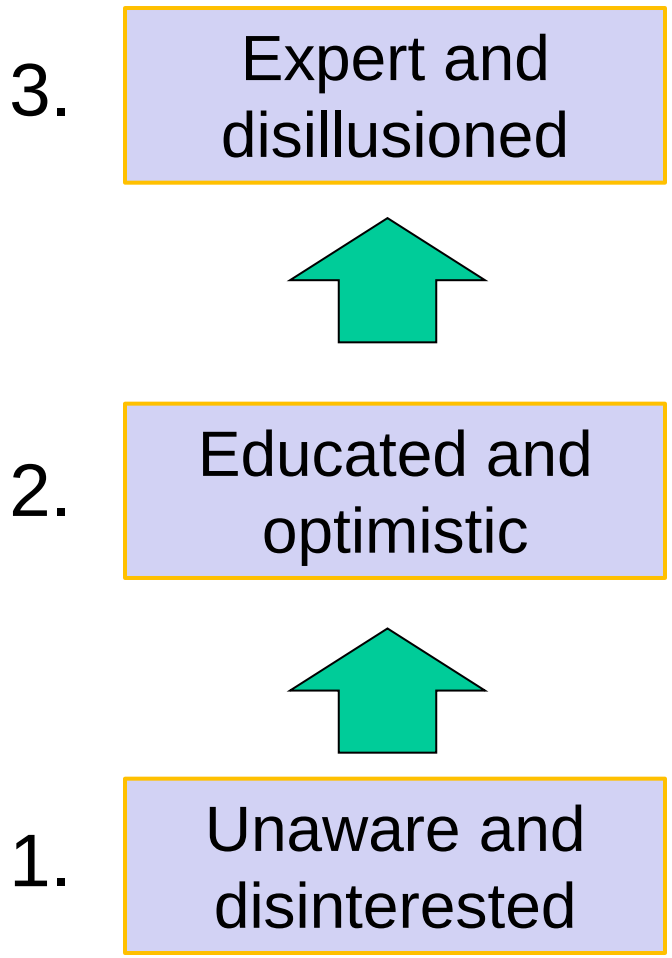
1. What does the little padlock *really* mean.
2. How to *properly* configure mod_ssl.
3. How to move and install certificates and private keys.
4. What .pem, .cer, .crt, .der, .p12, .p7s, .p7c, .p7m, etc mean.
5. How to reformat PKI files.
6. How to enable client authentication during mod_ssl configuration,
7. How to dump BER formatted ASN.1 stuff.
8. How to manually follow a certificate chain.
9. The risks of configuring SSL stuff such that it automatically starts during reboot.
10. How to extract certificates from PKCS7 files, etc.

Yahoo HCISec post – part 6

… and

11. How to make PKCS12 files.
12. How to use the OpenSSL utilities.
13. What happens if a key is revoked.

Stages of security learning
Revealing a deeper problem

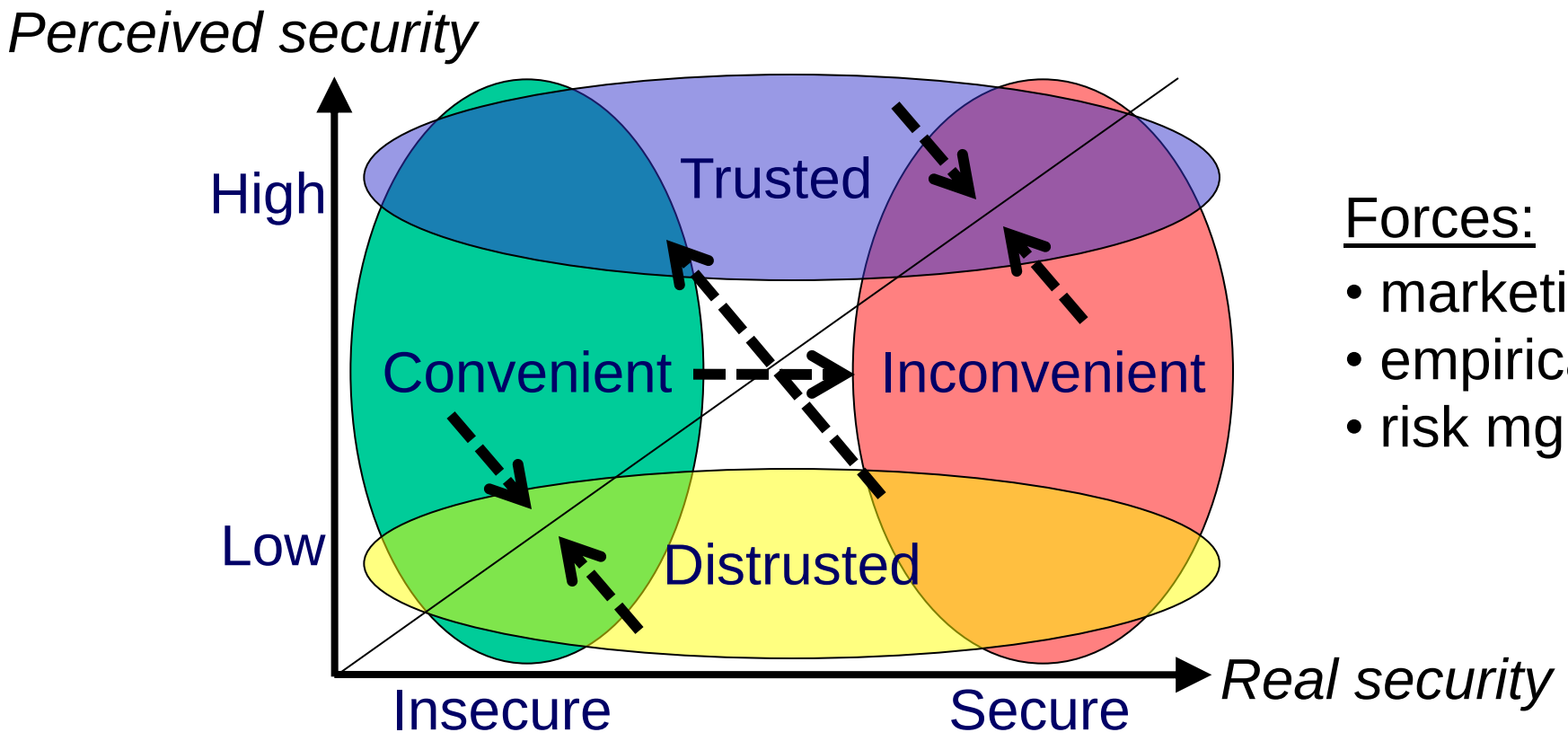


- *This is far more complex than I first thought. I actually don't think this can work.*
- *I understand it now, it's great, and I know how to operate it*
- *I don't understand it, and I don't want to know about it. Why can security not simply be transparent?*

The Fake Security Industry

- Security is big business
- Security solutions don’t produce anything
- Security solutions give a cosy warm feeling
- Security solutions that don’t work can still give that cosy warm feeling
- That’s great, lets sell security solutions that don’t work
  - PKI, Trusted Computing, Crypto AG, OpenID
- Understanding what doesn’t work is a challenge

Perception and reality; The subjective perspective

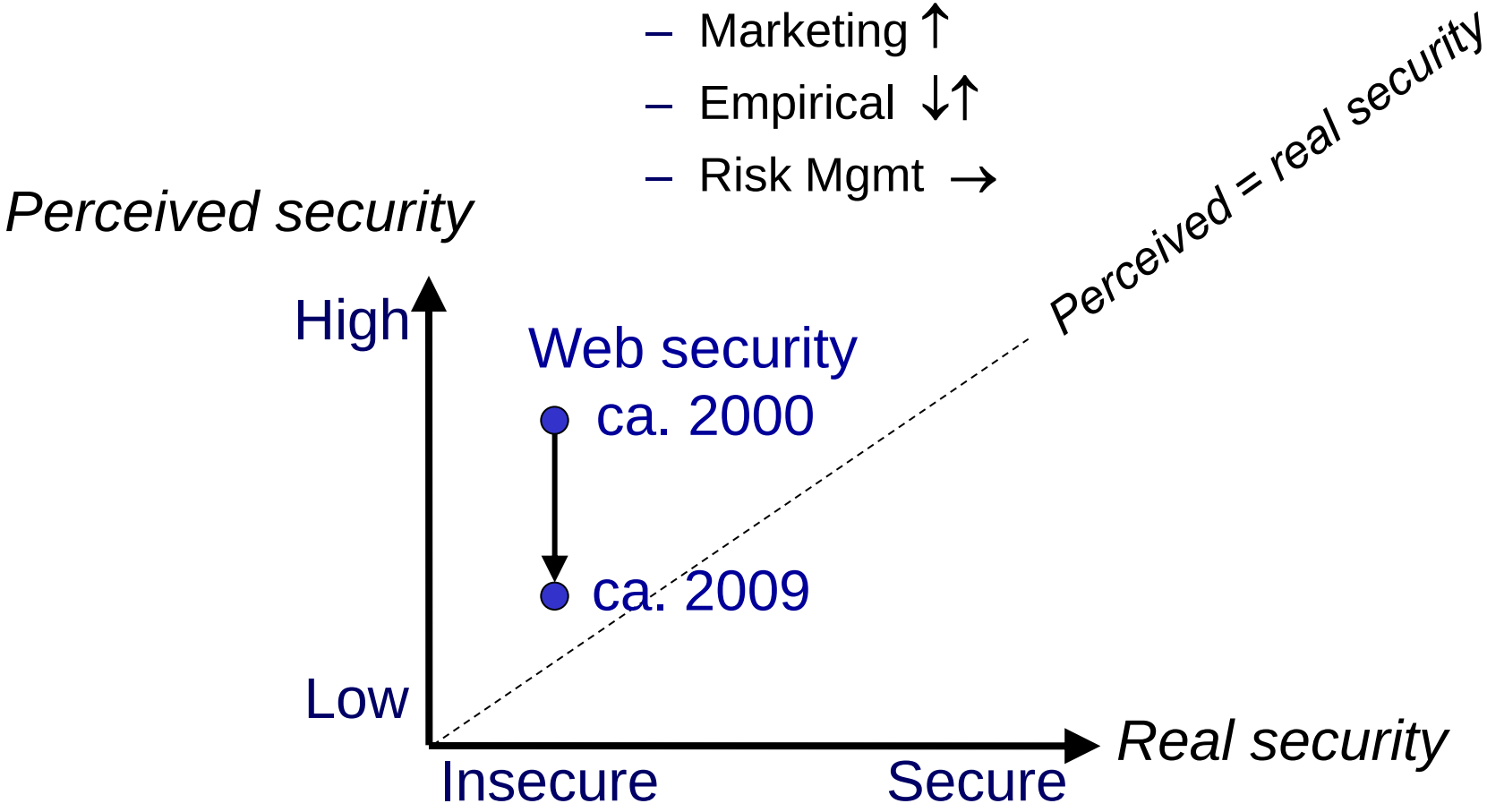


Forces:

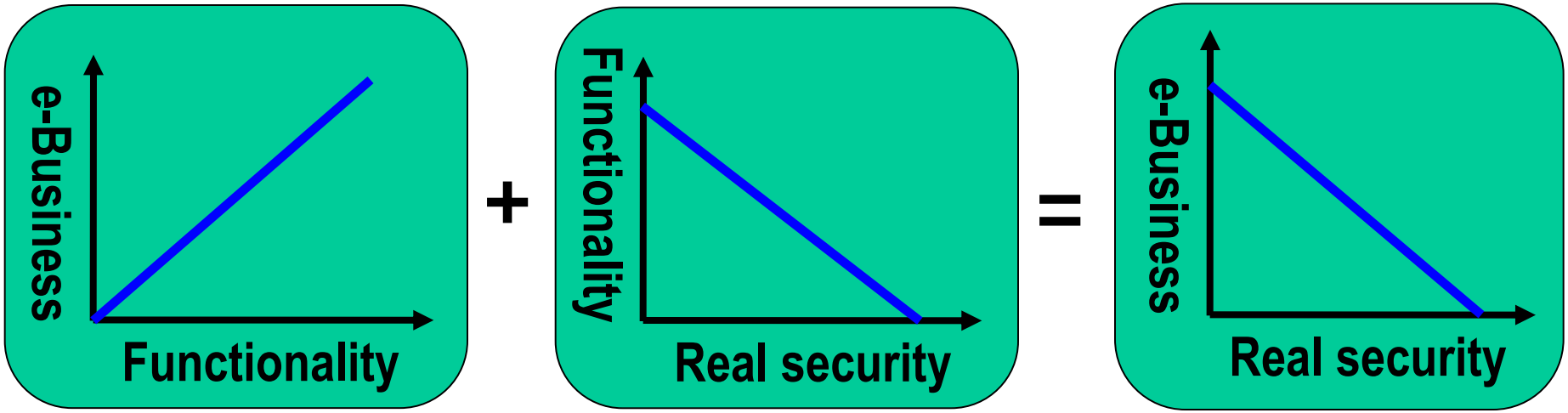
- marketing
- empirical
- risk mgmt

Real and perceived security

- Opposing forces
  - Marketing ↑
  - Empirical ↓↑
  - Risk Mgmt →

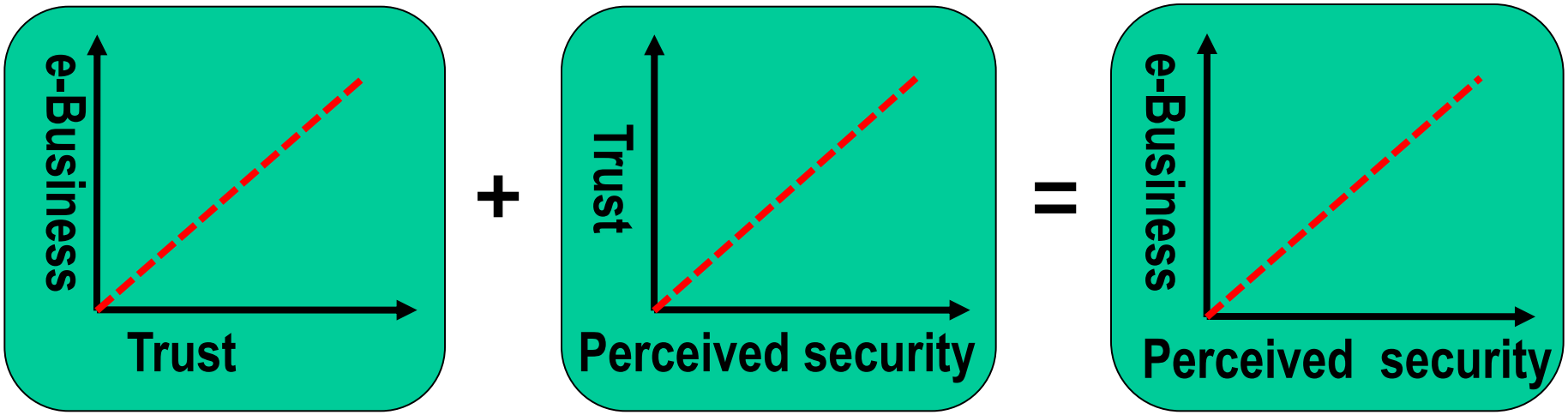


Real security is bad for e-business



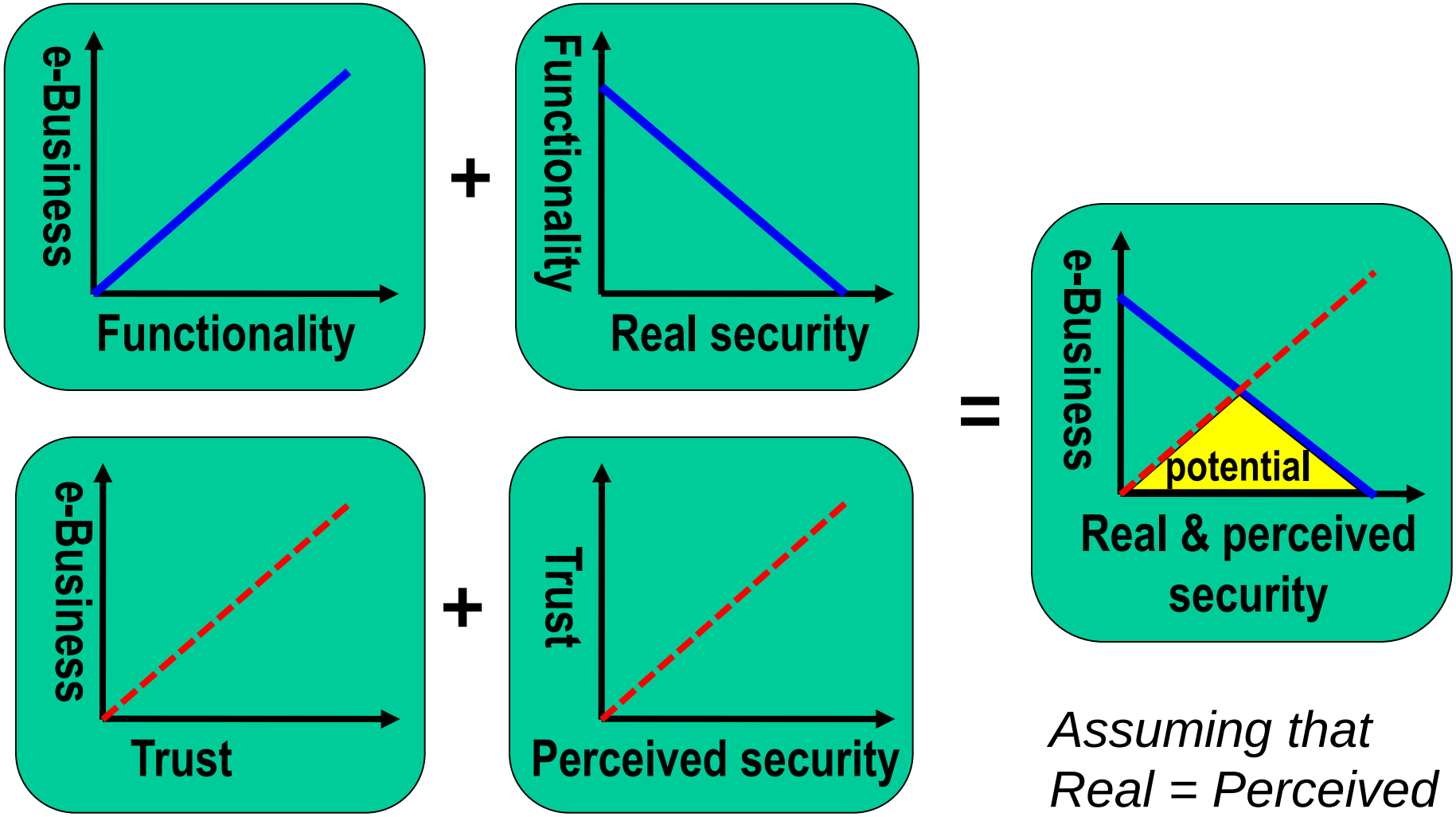
- e-business revolution not possible with real security
- Thank God the Internet isn't secure

Perceived security is good for e-business



- e-business growth needs perceived security

e-Business growth potential



Assuming that Real = Perceived

Can a nice UI make security tools easy to use?

- **Problem lies deeper:**
  - **“key” cues the wrong mental model**
  - **Meaning of “public” and “private” is different from everyday language**
  - **Underlying model too complex**
- **Solutions?**
  - **Automatic transparent solutions where that is possible**
  - **Simplify model/language**
  - **Build systems based on simple intuitive models**
  - **Require security learning when necessary**
  - **Do not allow fake security!**

Sustaining v/ Disruptive Approach

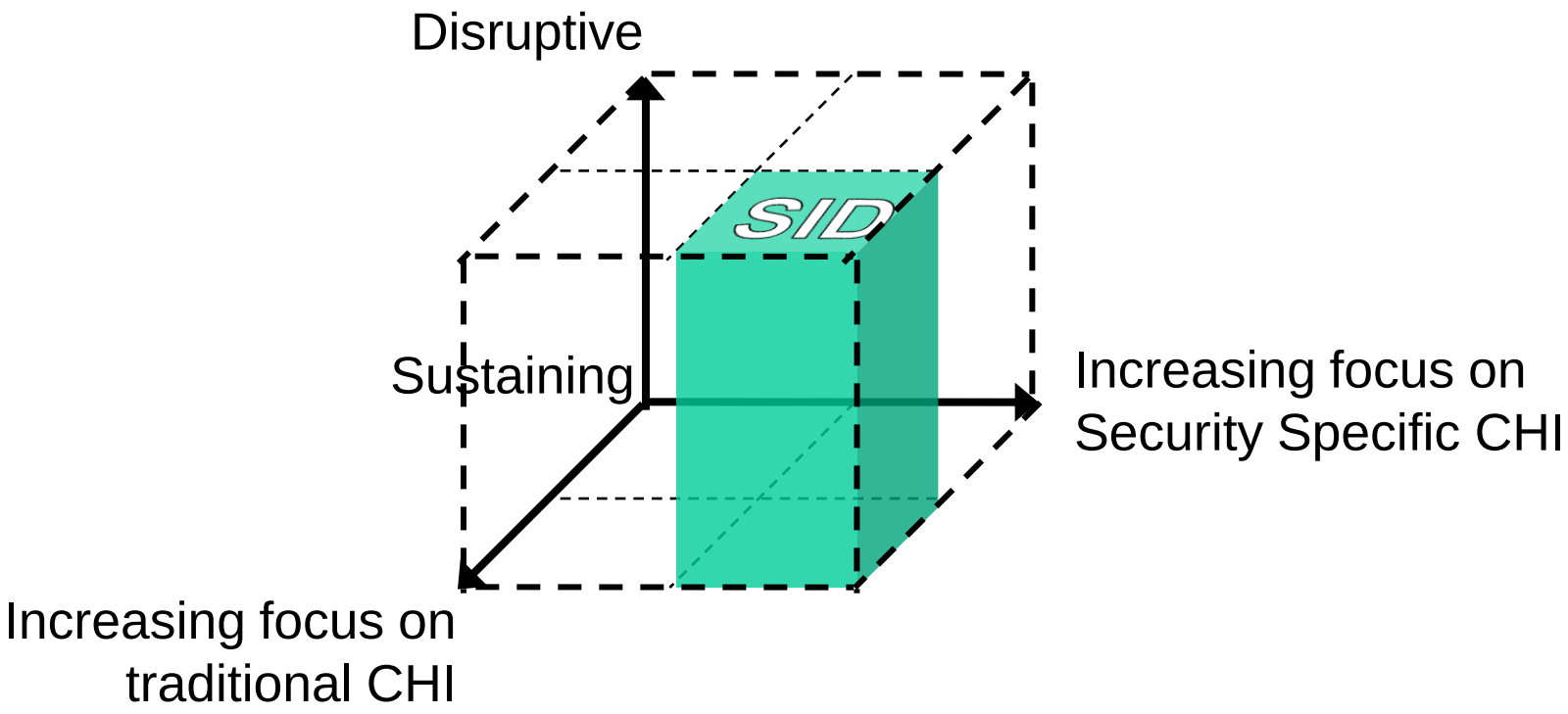
Sustaining approach

- Existing security building blocks have adequate potential for good usability
- Optimize interface

Disruptive approach

- Existing security building blocks represent an obstacle to usability
- Replace existing security building blocks with radically new ones with better potential for usability

Security Interaction Design



Usability in identity management

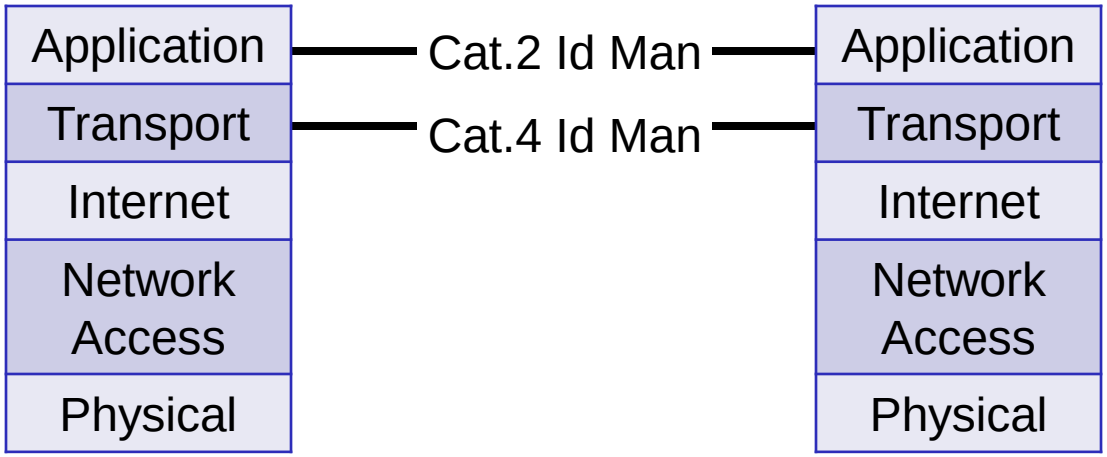
- Four categories of identity management

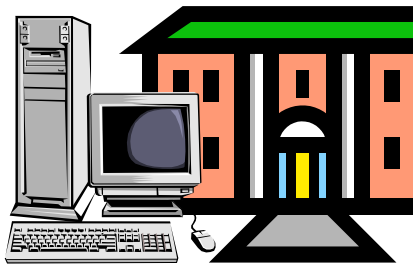
(1) Mgmt of user IDs and credentials on SP side	(2) Mgmt of user IDs and credentials on user side
(3) Mgmt of SP IDs and credentials on SP side	(4) Mgmt of SP IDs and credentials on user side

- Only type 1 is traditionally considered part of IAM
- Types 2 &4 are relevant for security usability

Identity Management for Users

User





Service Provider

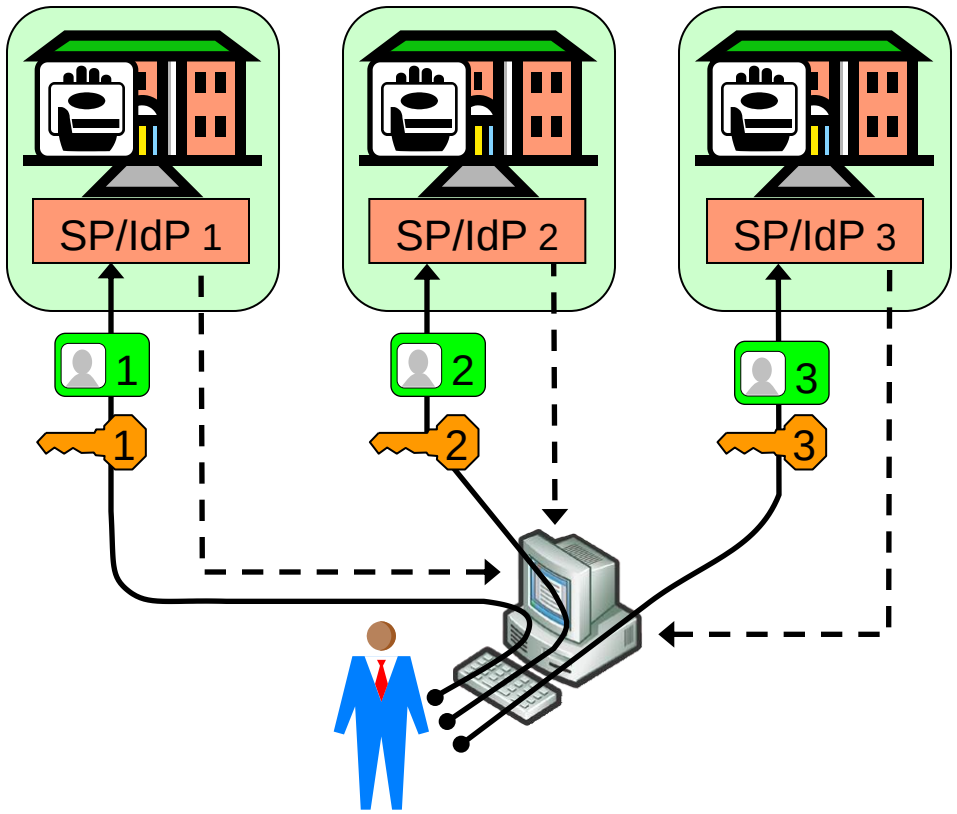
- Cat.2: Mgmt of user Ids and creds. on user side
- Cat.4: Mgmnt of SP Ids and creds. on user side

Category (2): Mgmt of User Ids on the User Side

- Insufficient attention from industry and research
- No technology support
  - Password management device
  - Users have to improvise
- Policies are silo specific
  - SPs give policy advice about passwords for their service, but not about handling passwords for multiple services, e.g. same password for multiple services

You're on your own!

The Traditional Silo Model



Legend:

SP

IdP

Identity domain

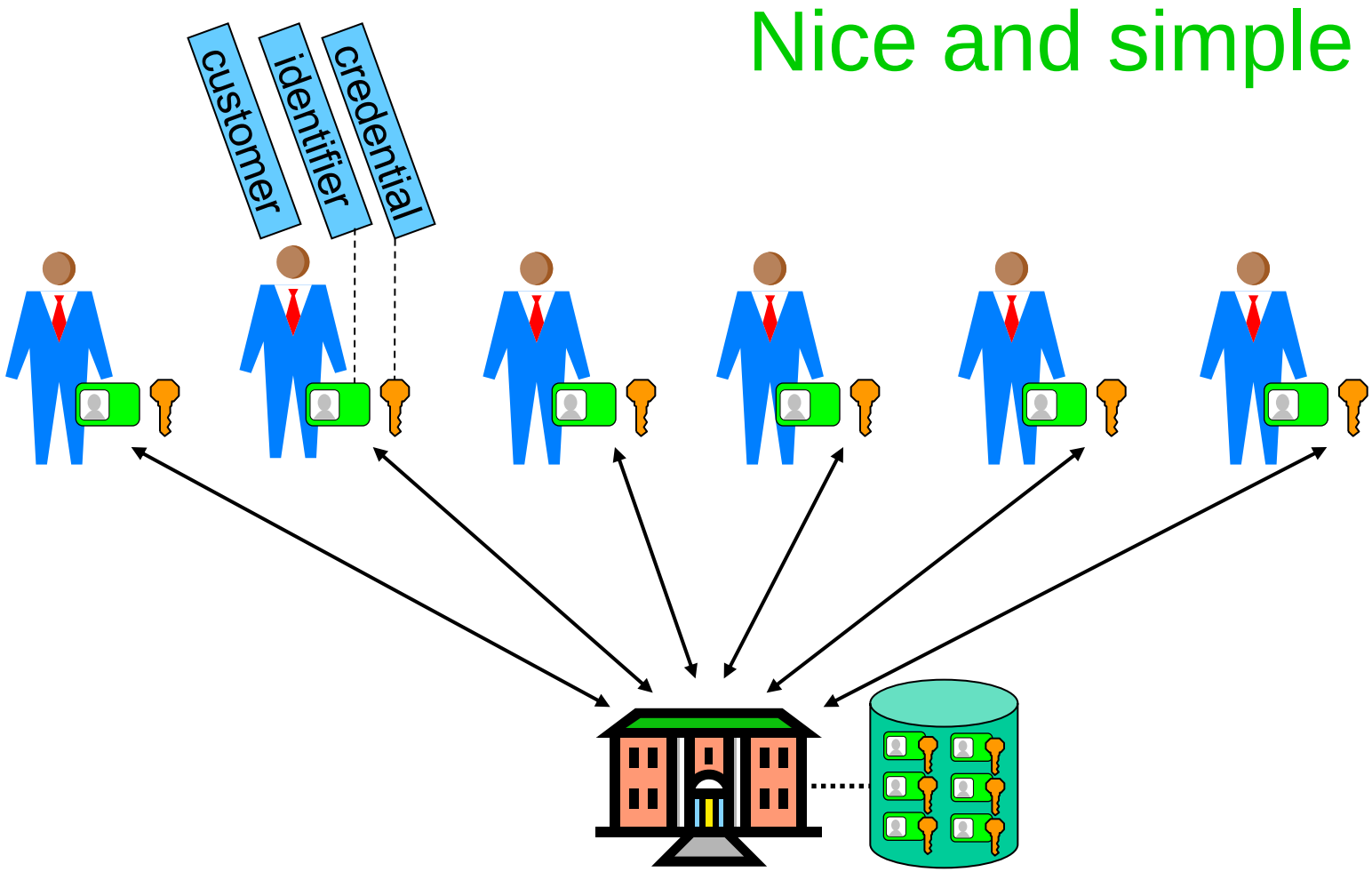
User identifier managed by IdP #

Authentication token managed by IdP #

User logon

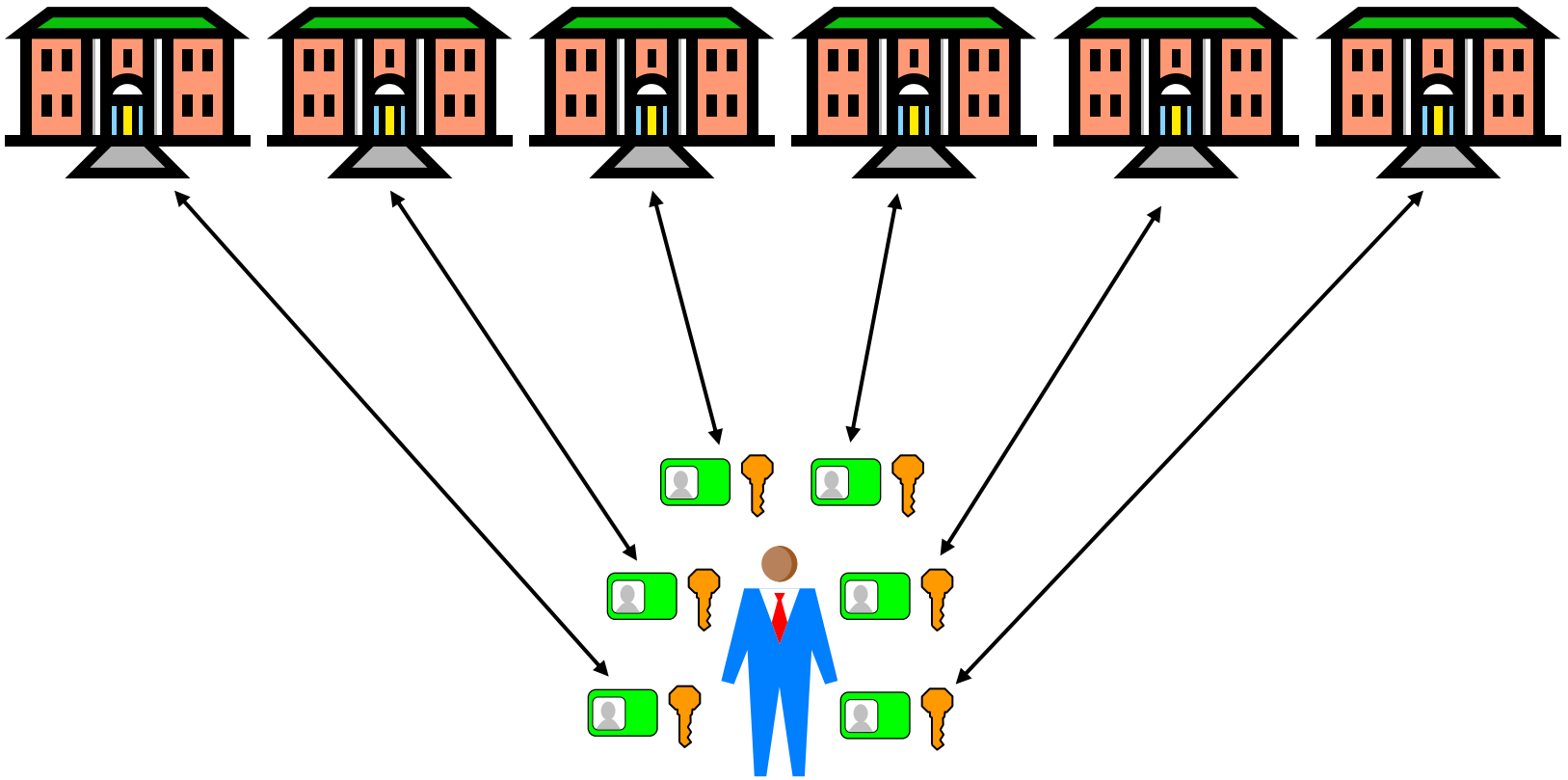
Service provision

Imagine you're a service provider

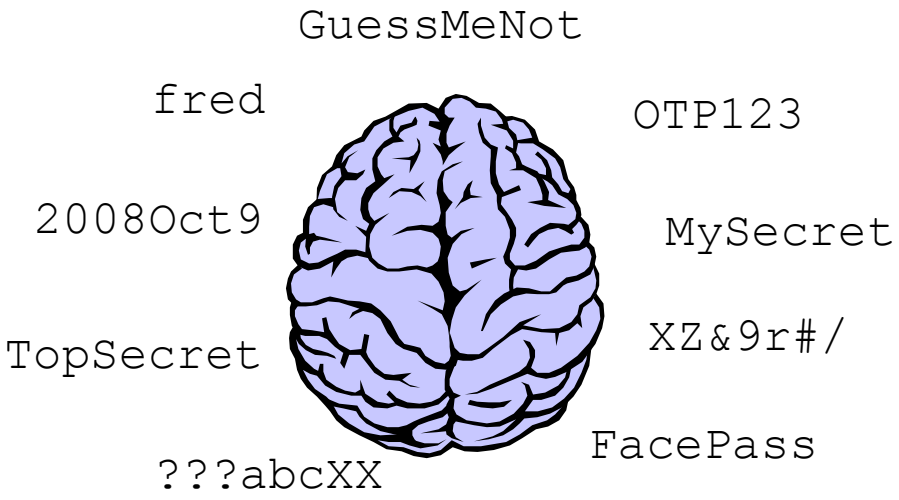


Imagine you're a customer

It's a usability nightmare



Tragedy of the commons



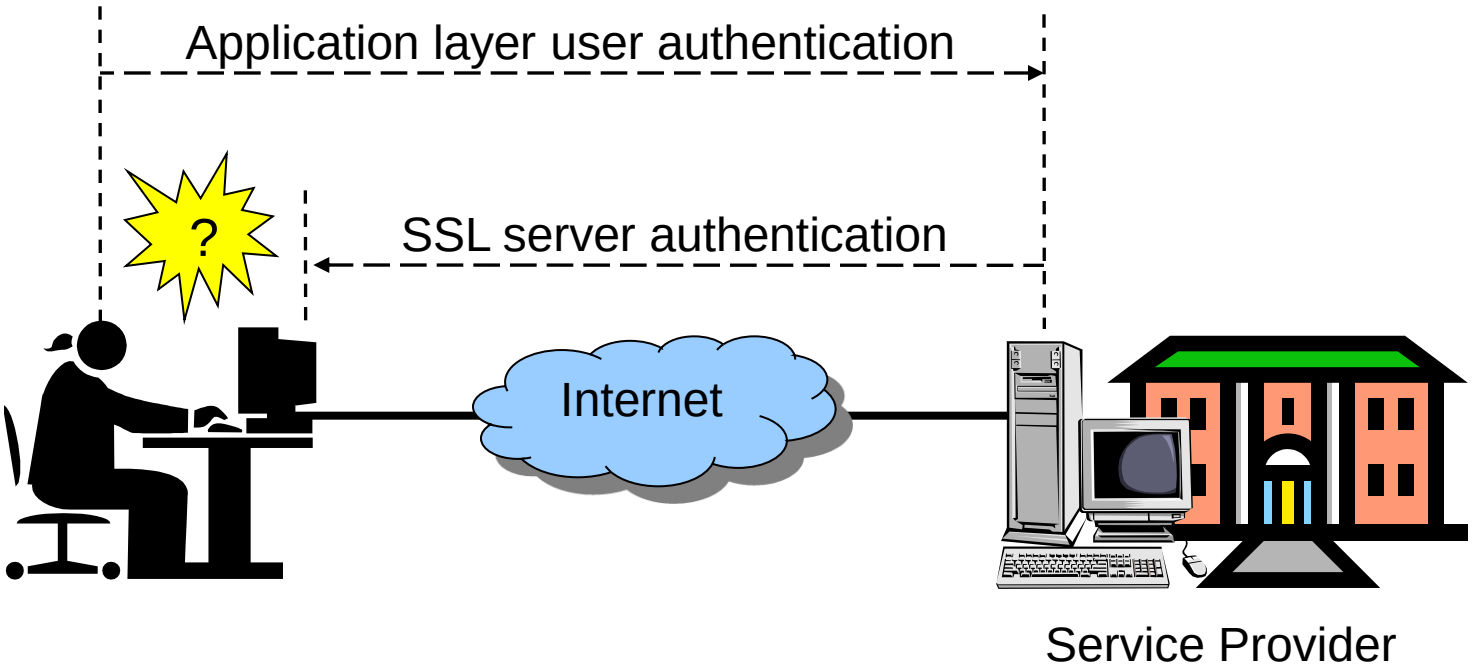
Category (4): Mgmt of SP Ids on the User Side

- The industry has made it transparent
- Automated mechanistic authentication
- Semantically meaningless authentication

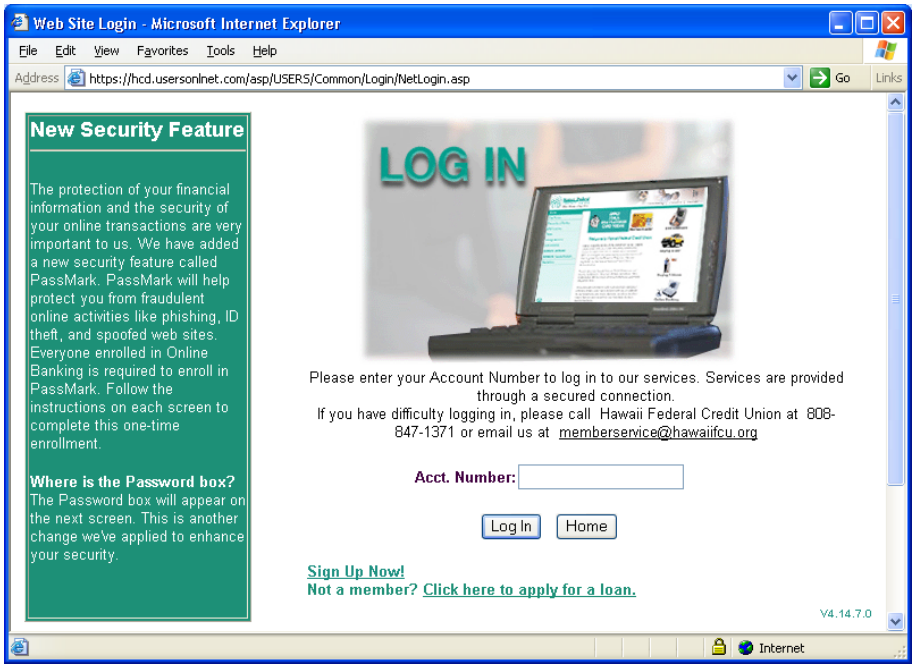
You're never told!

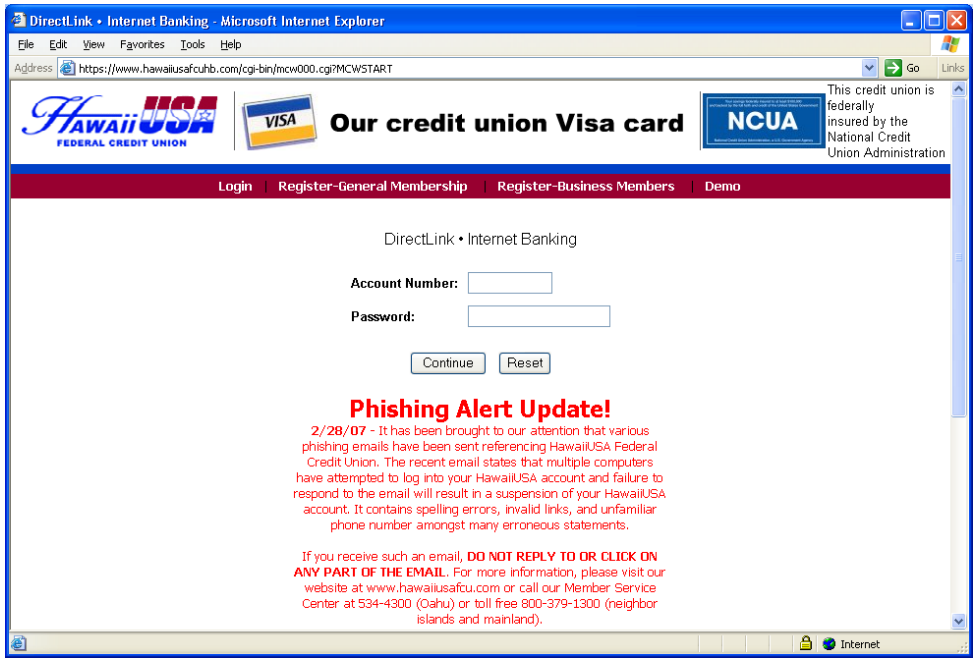
- Philosophical question: can authentication be automated?

Usability of server authentication



A phishing example: Hawaii Federal Credit Union





Genuine bank login

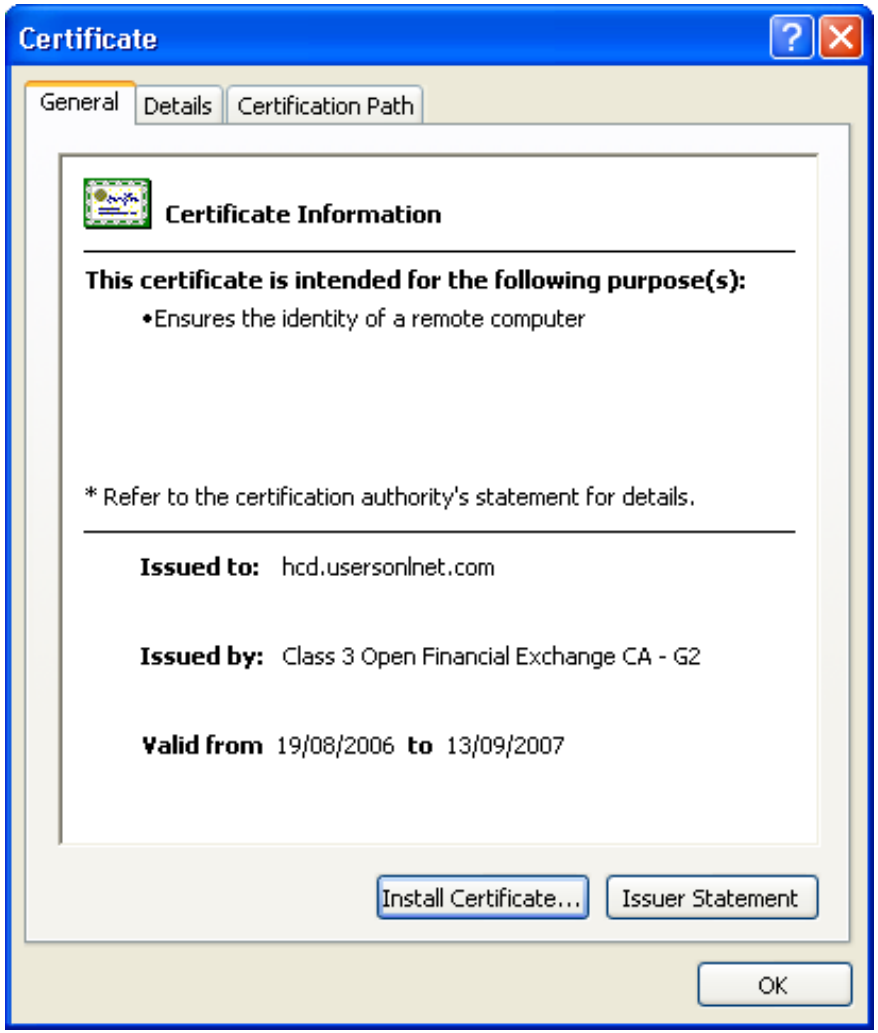
https://hcd.usersonlnet.com/asp/USERS/Common/Login/NettLogin.asp

Fake bank login

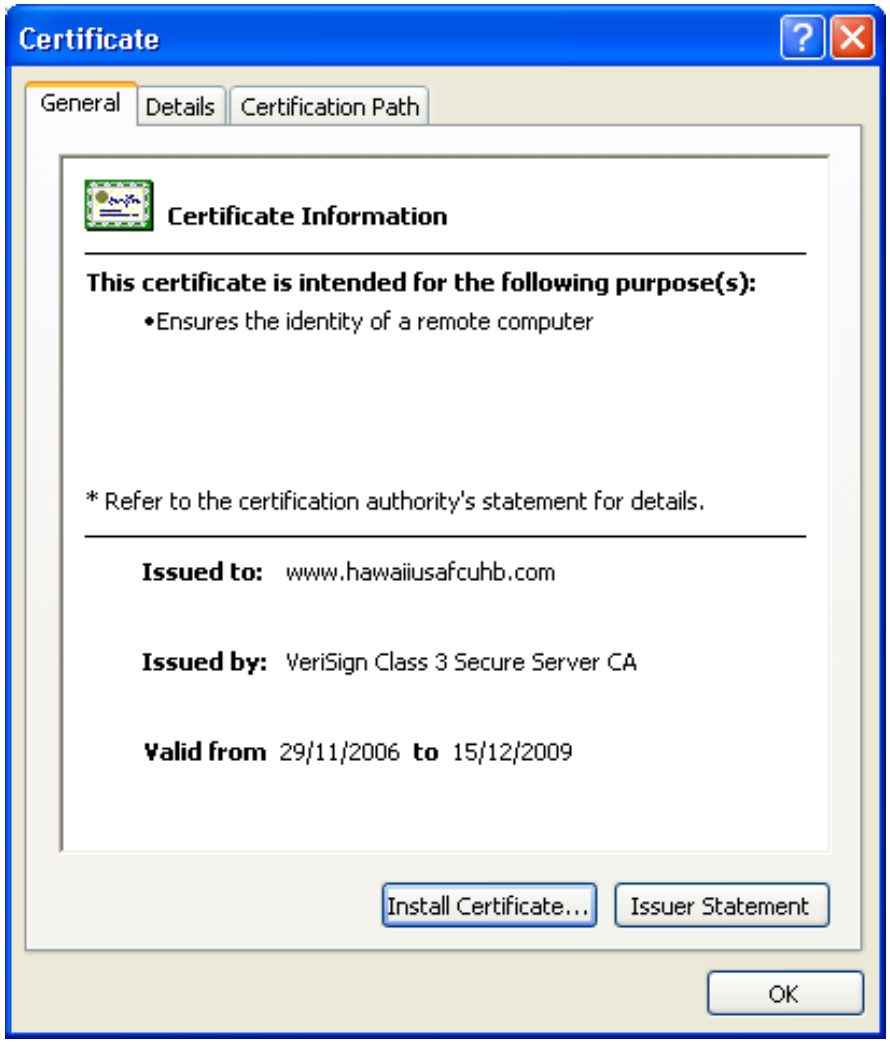
https://hawaiiusafcuhb.com/cgi-bin/mcw00.cgi?MCWSTART

UNIK

Certificate comparison 1

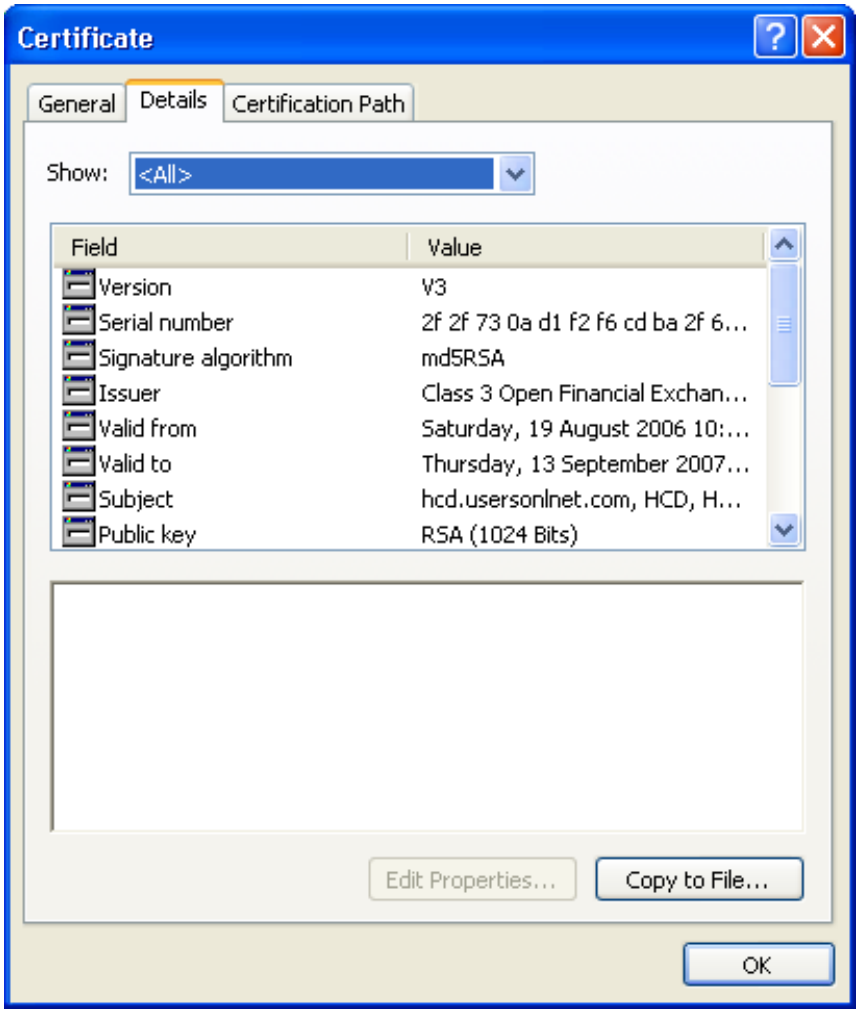


Genuine certificate

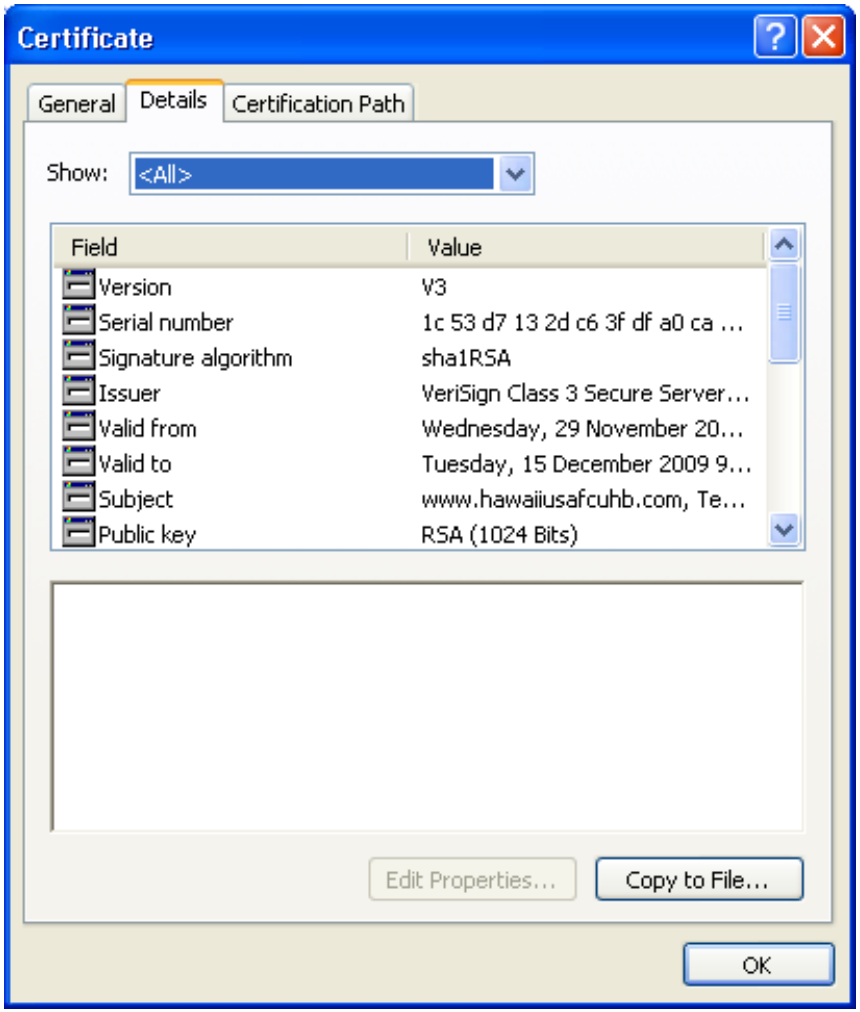


Fake certificate

Certificate comparison 2

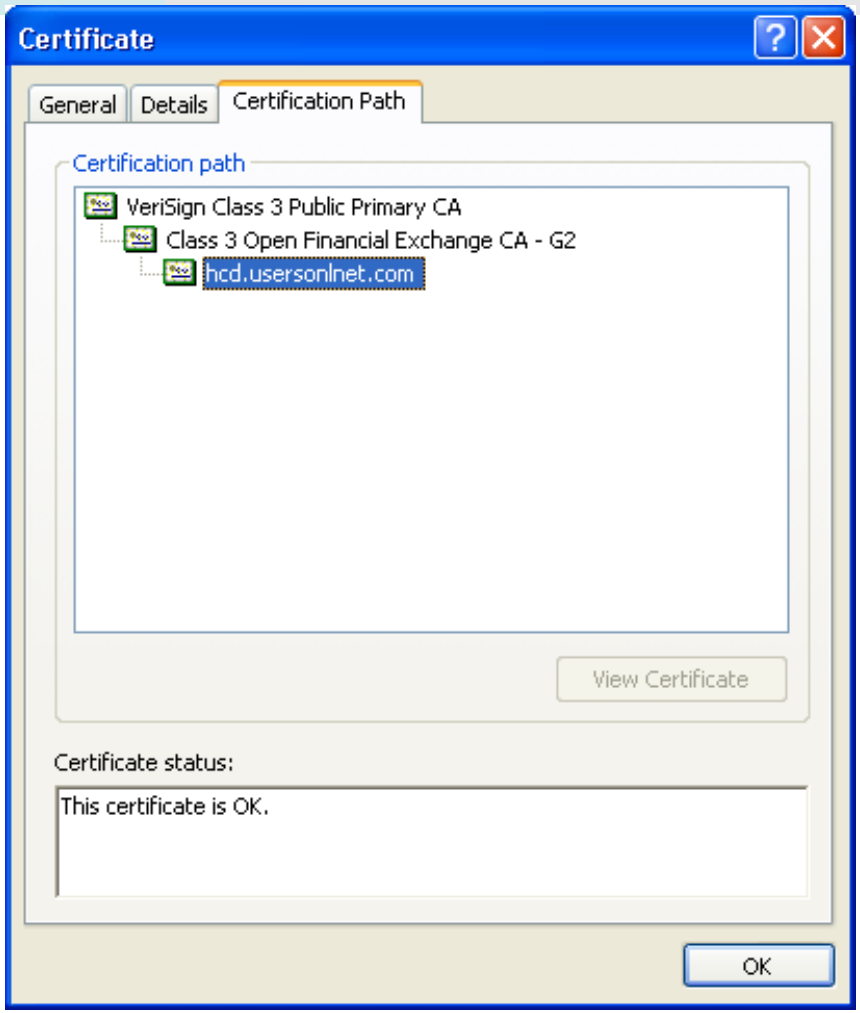


Genuine certificate

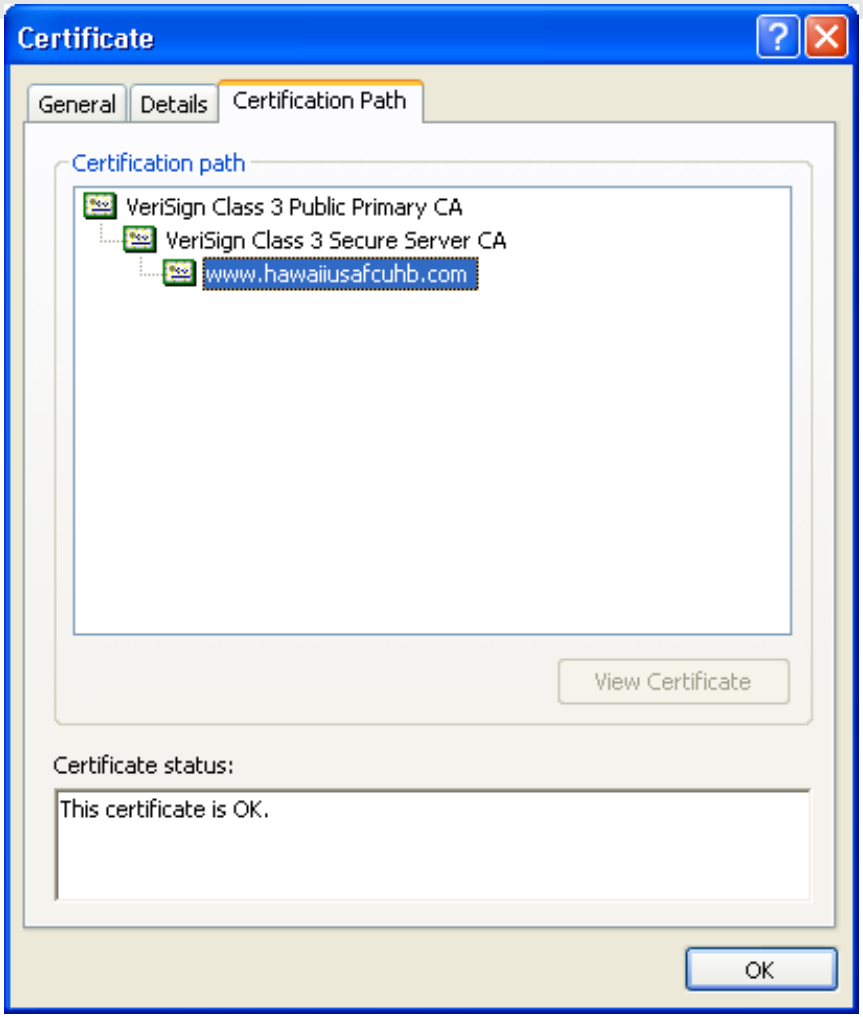


Fake certificate

Certificate comparison 3



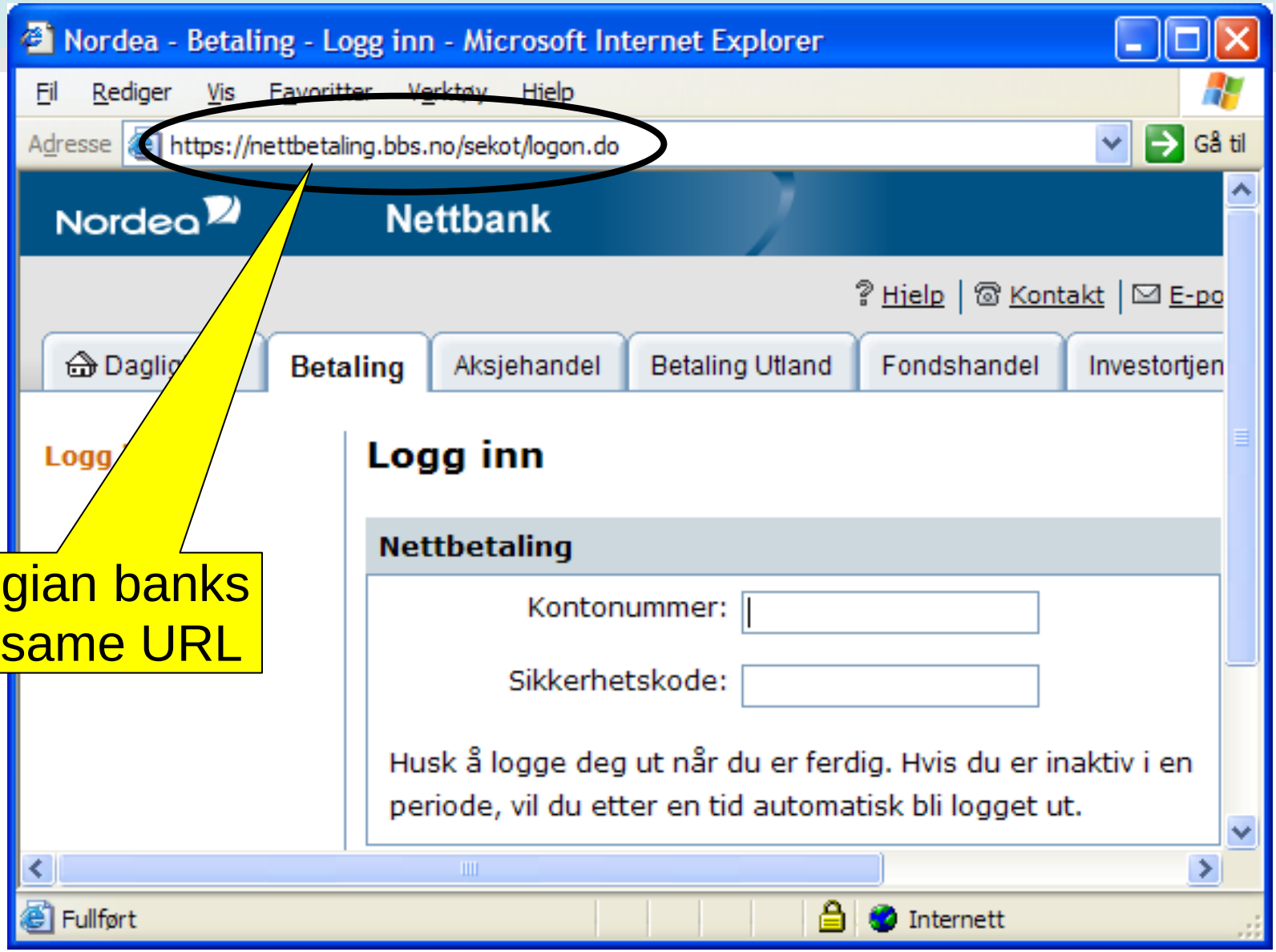
Genuine certificate



Fake certificate

UNIK

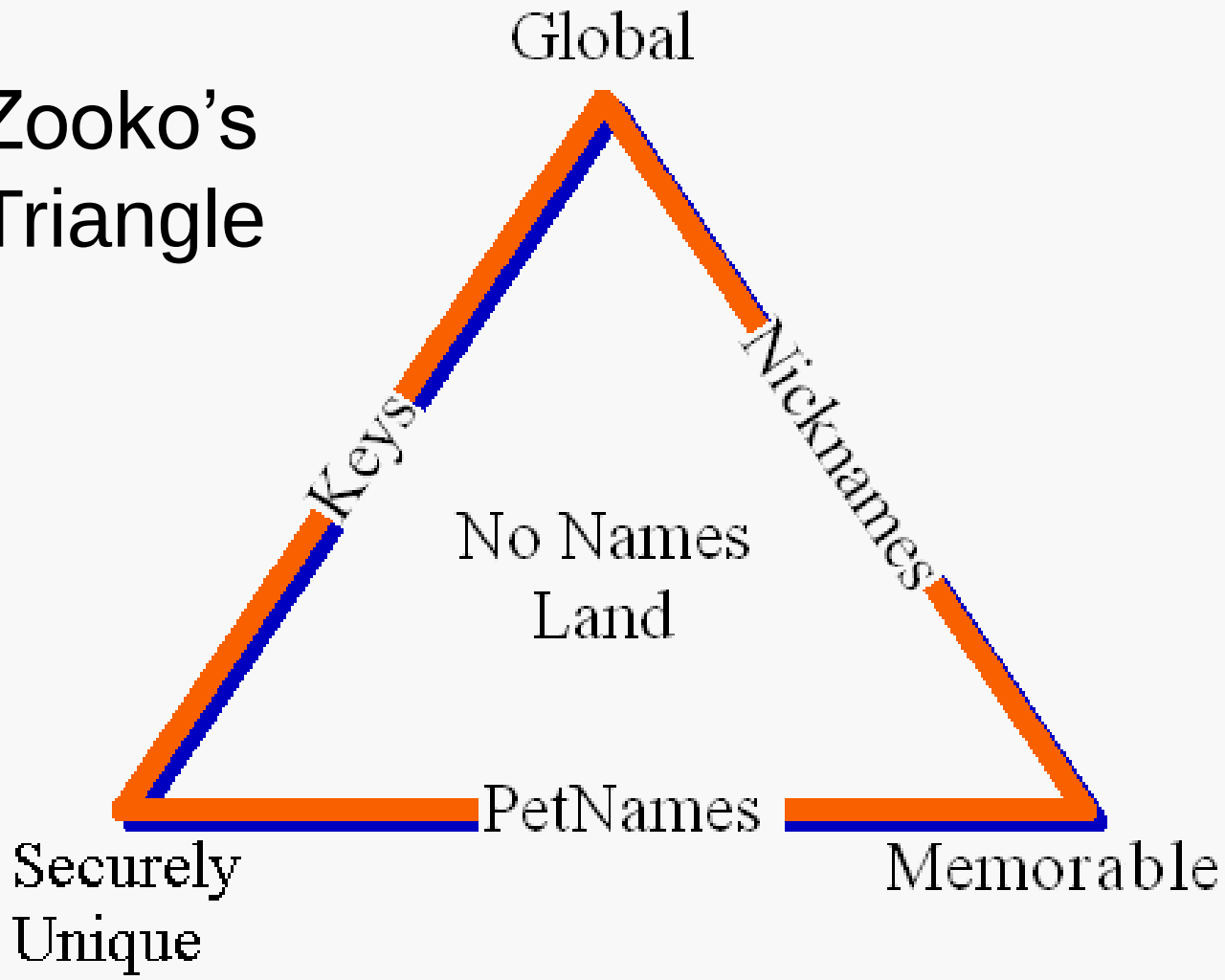
Unintended vulnerability



All Norwegian banks have the same URL

There is hope: Petname Systems

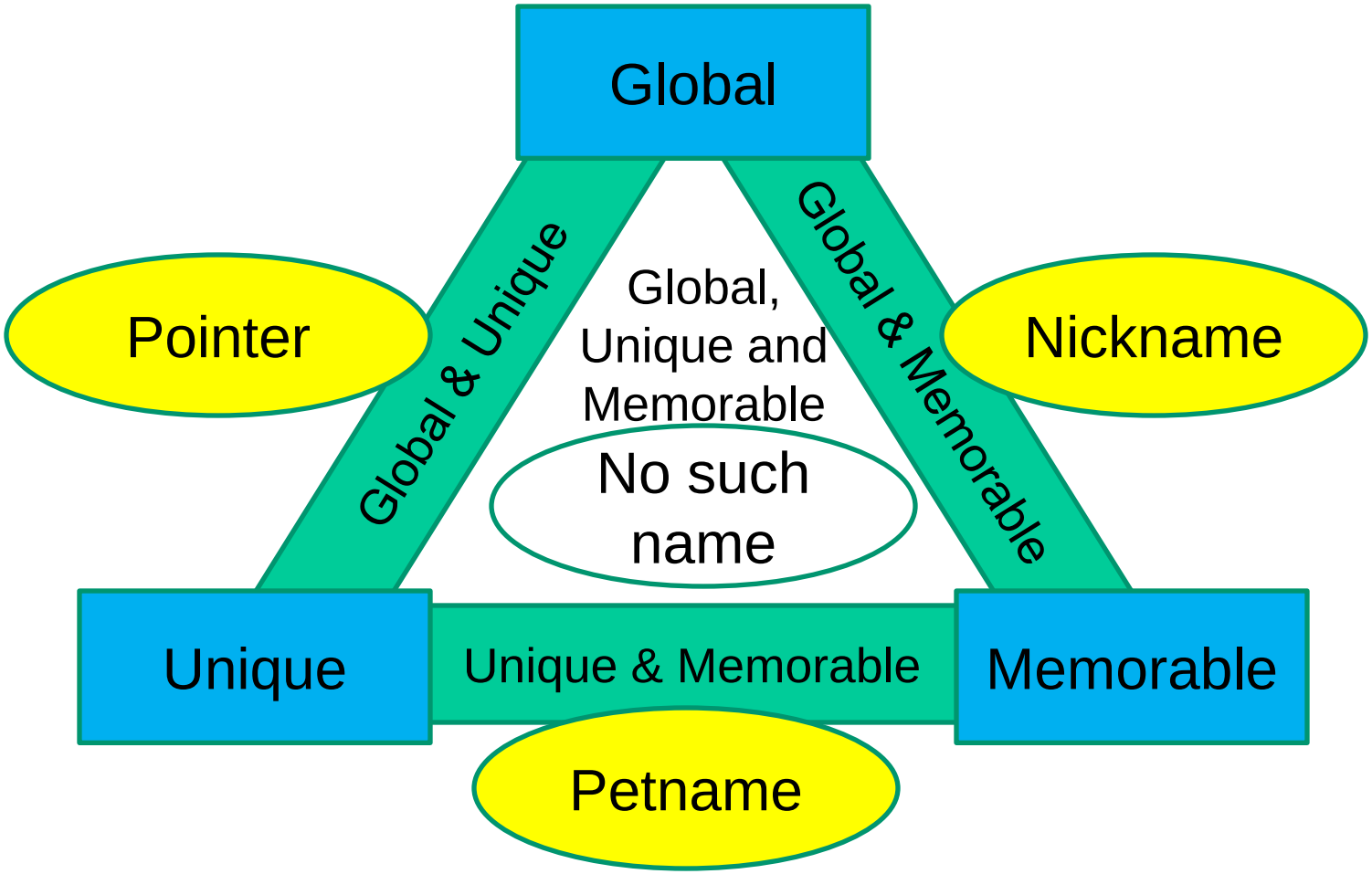
Zooko's Triangle



Zooko's triangle

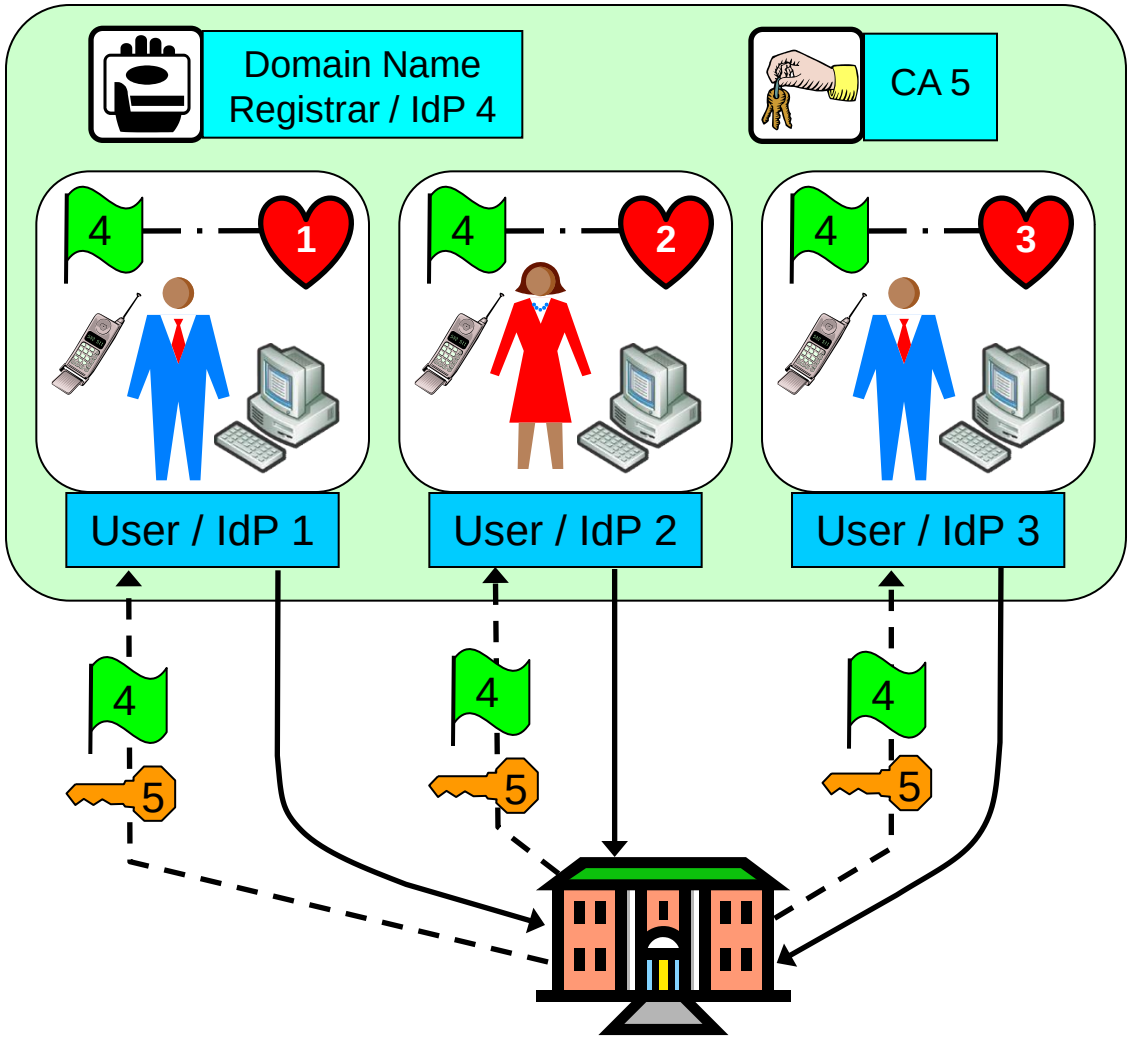
- Desirable properties of an identifier:
  - Global
  - Unique
  - Memorable (passing bus test)
- Identifiers can only have 2 of the properties.
  - Global & Unique: **Pointer**
    - e.g. URL: *www.pepespizza.co.nz*
  - Global & Memorable: **Nickname**
    - e.g. *Pépés Pizza*
  - Unique & Memorable: **Petname**
    - e.g.: *My Wellington Pizza*

Modern terminology for Zooko's Triangle



Petnames in server authentication

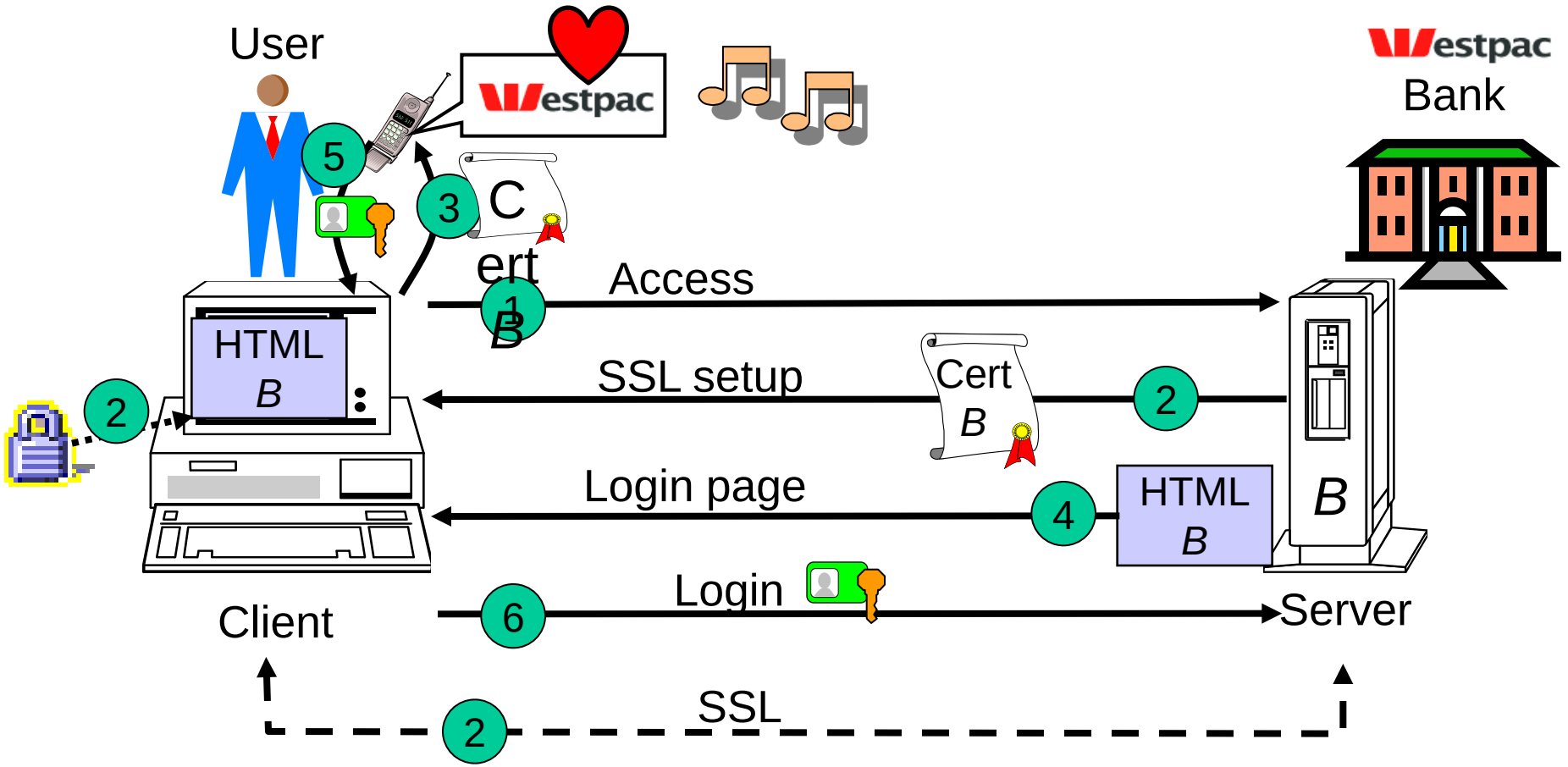
User Centric model



Legend :

- Identity domain
- Domain name issued by IdP #
- Petname defined by user #
- PDA / mobile
- SP entity
- Domain name registrar / IdP
- CA
- Auth. token issued by CA #
- Service access
- SP authentication
- Identifier mapping

User-centric server authentication

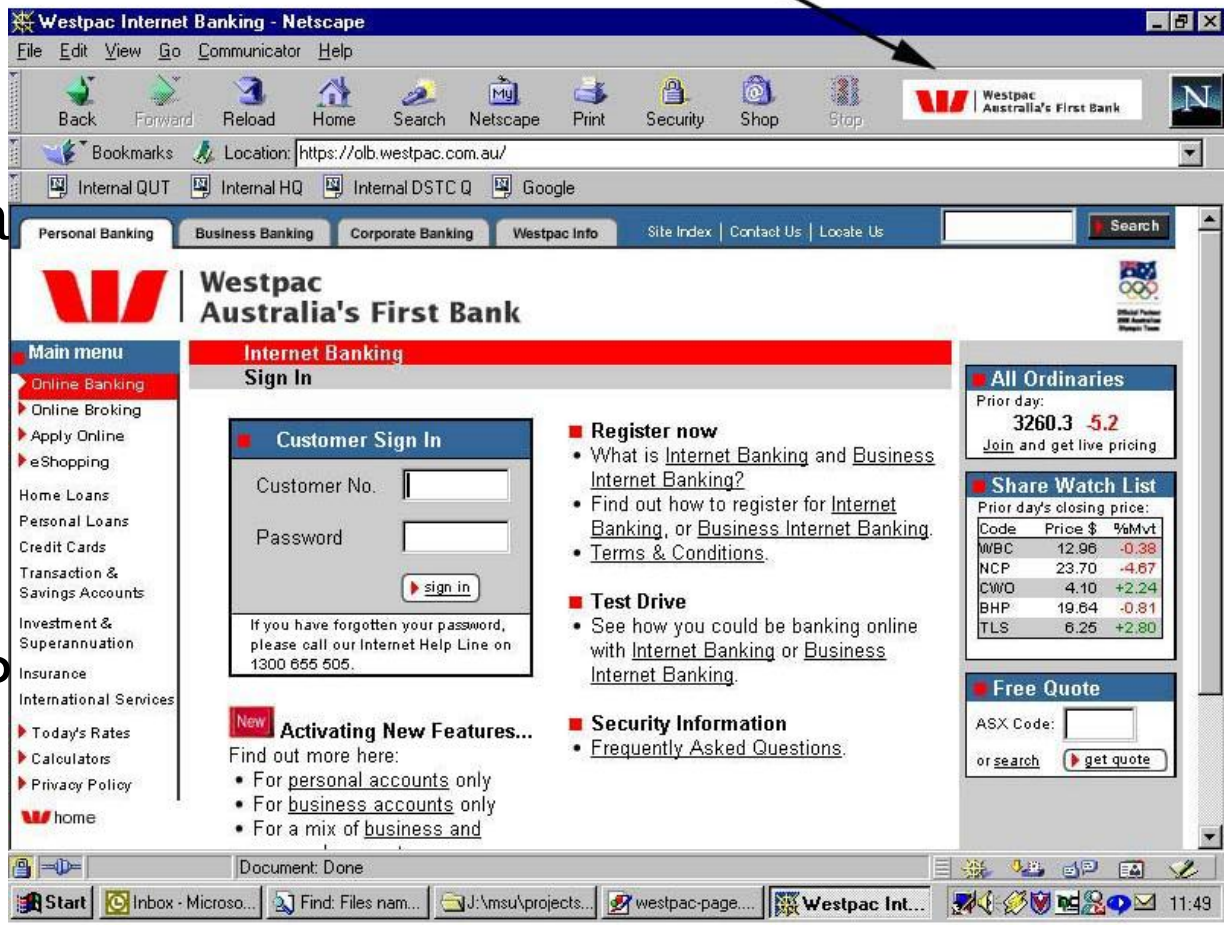


SP identity management

Petname system in Mozilla TrustBar

Personalised graphical logo and/or sound as site identifier

- Toolbar for the Mozilla and Firefox browsers
- Server certificates personalised by user
- Personal graphics or sound played when SP certificate recognised by browser



Large, expensive, polluting entities

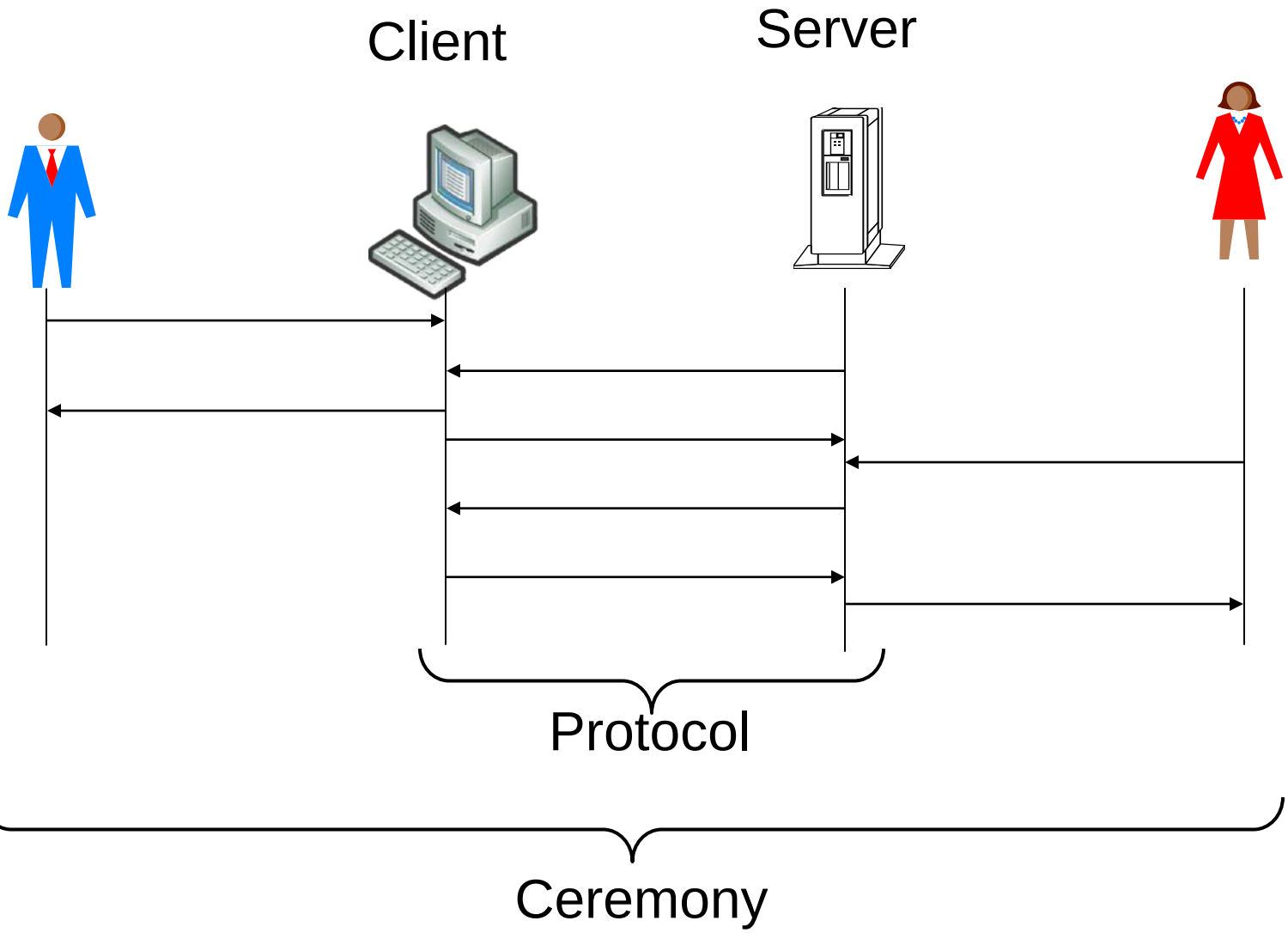
"Humans are incapable of storing high-quality cryptographic keys, and the have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment.) It is astonishing that these devices continue to be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations."

[C. Kaufmann, R. Perlman & M. Speciner: *Network Security*]

Ceremony
Including humans in formal protocol

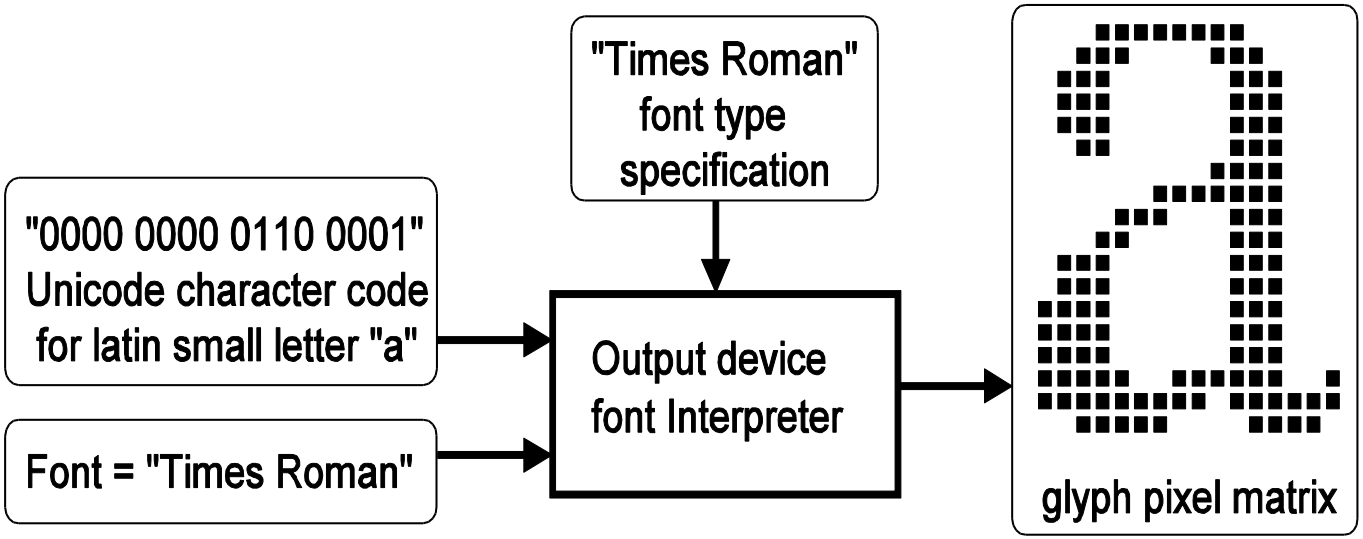
- Humans obviously play a role in security procedures
- Ceremony is the idea of formally including humans in protocol design, analysis and verification
- Promoted by Carl Ellison of Microsoft

Ceremony – Extended Protocol



Digital signatures on documents

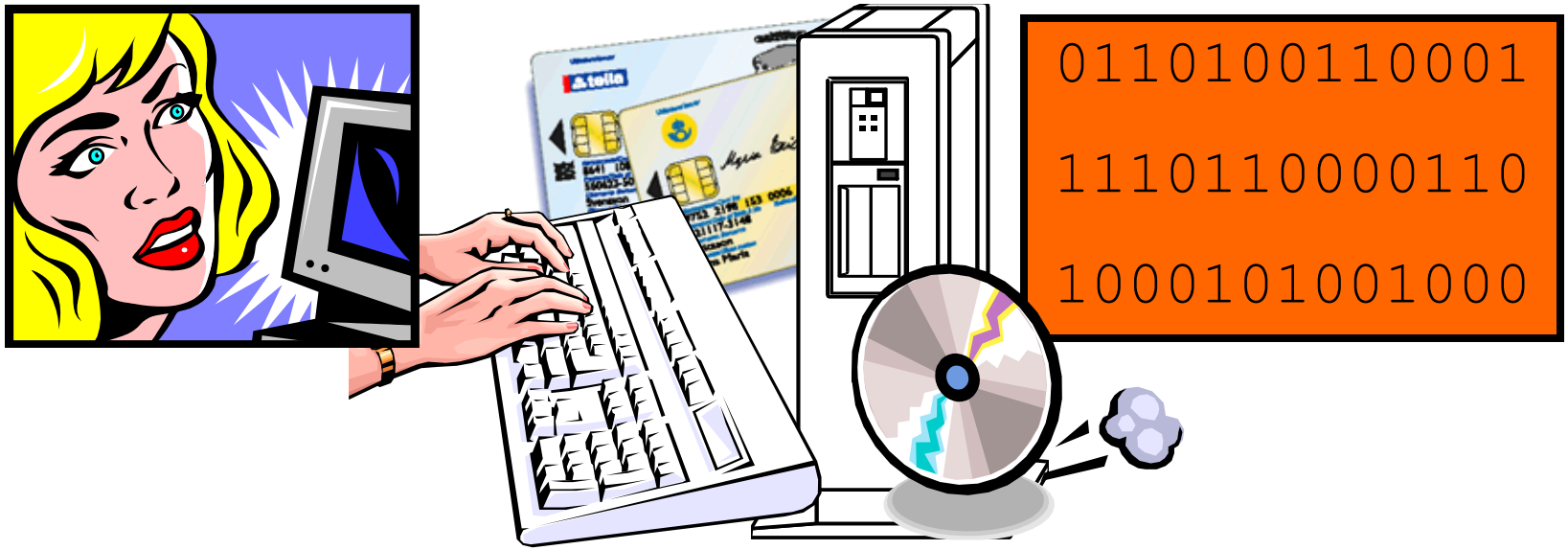
- Users erroneously believe they sign semantic content
- Digital signature applies to the binary representation of digital documents
- Complex processes needed to transform binary form into semantic content
- Many attacks possible, e.g. font replacement



WYSIWYS
What You See Is What You Sign

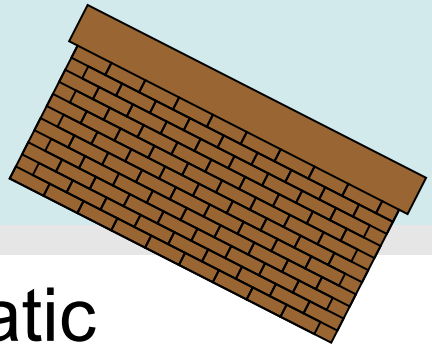
- WYSIWYS means that the semantic interpretation of a signed message cannot be changed. In particular this also means that a message cannot contain hidden info that the signer is unaware of, and that can be revealed after the signature has been applied.
- WYSIWYS is a desirable property of digital signatures that is difficult to guarantee because of the increasing complexity of modern computer systems.

There is more than just a pen between a signer and digital document



- “What You See Is Not Always What You Sign” by Jøsang, Povey & Ho, AUUG 2002
- Describes many ways of changing semantic representation of the same digital content

Firewalls



- "Firewall" seems to indicate something static
  - Unfortunate metaphor
- "Traffic guard" or "Gatekeeper" would be a better metaphor
  - Checks who goes in and out

- Your computer can be a busy place
  - Many processes send and receive traffic
  - Difficult to automate gatekeeper function

- Difficult to configure
- Identities of local and remote processes is a problem

Security Usability in Practice

- Aspects of security usability fairly well understood in the research community
- Literature ignored by implementers
- Security interaction design is challenging
  - New principles
  - Interdisciplinary
- Research required to improve and validate security interaction design methods
- No security system is complete before usability aspects have been considered

Biometrics and usability

- Why use biometrics?
  - convenient as cannot be lost or forgotten
  - provides for positive authentication
    - Difficult to copy, share, and distribute
    - Passwords and token can be loaned to others
    - Require the person being authenticated to be present at the time and point of authentication.
  - increasingly socially acceptable
  - becoming less expensive
  - considered very effective as part of a two-factor authentication scheme.
  - can also be used for identification

Biometrics: Characteristic requirements

- **Universality**:
  each person should have the characteristic;
- **Distinctiveness**:
  any two persons should be sufficiently different in terms of the characteristic;
- **Permanence**:
  the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time;
- **Collectability**:
  the characteristic can be measured quantitatively.

Biometrics: Practical considerations

- Performance:
  - the achievable recognition accuracy and speed,
  - the resources required to achieve the desired recognition accuracy and speed,
  - the operational and environmental factors that affect the accuracy and speed;
- Acceptability:
  - the extent to which people are willing to accept the use of a particular biometric identifier (characteristic)
- Circumvention:
  - how easily can the system be fooled

Biometrics: Uses

- Where could biometric-based authentication be used?
  - workstation, network, and domain access,
  - single sign-on,
  - application logon,
  - data protection,
  - remote access to resources,
  - transaction security and
  - Web security

Biometrics
Security Considerations

- Biometrics are not secrets and are therefore susceptible to modified or spoofed measurements
- There is no recourse for revoking a compromised identifier
- Strategic Solutions
  - Liveness testing
  - Multi-biometrics

Biometrics
Privacy Considerations

- A reliable biometric system provides an irrefutable proof of identity
- Threatens individuals right to anonymity
  - Cultural concerns
  - Religious concerns
  - Violates civil liberties
- Strategic Solutions
  - Biometric cryptosystems
  - Transparency

Bometrics
Safety Consideration

- Biometric authentication can be a safety risk
  - Attackers might try to “steal” body parts
  - Subjects can be put under duress to produce biometric authenticator
- Necessary to consider the physical environment where biometric authentication takes place.

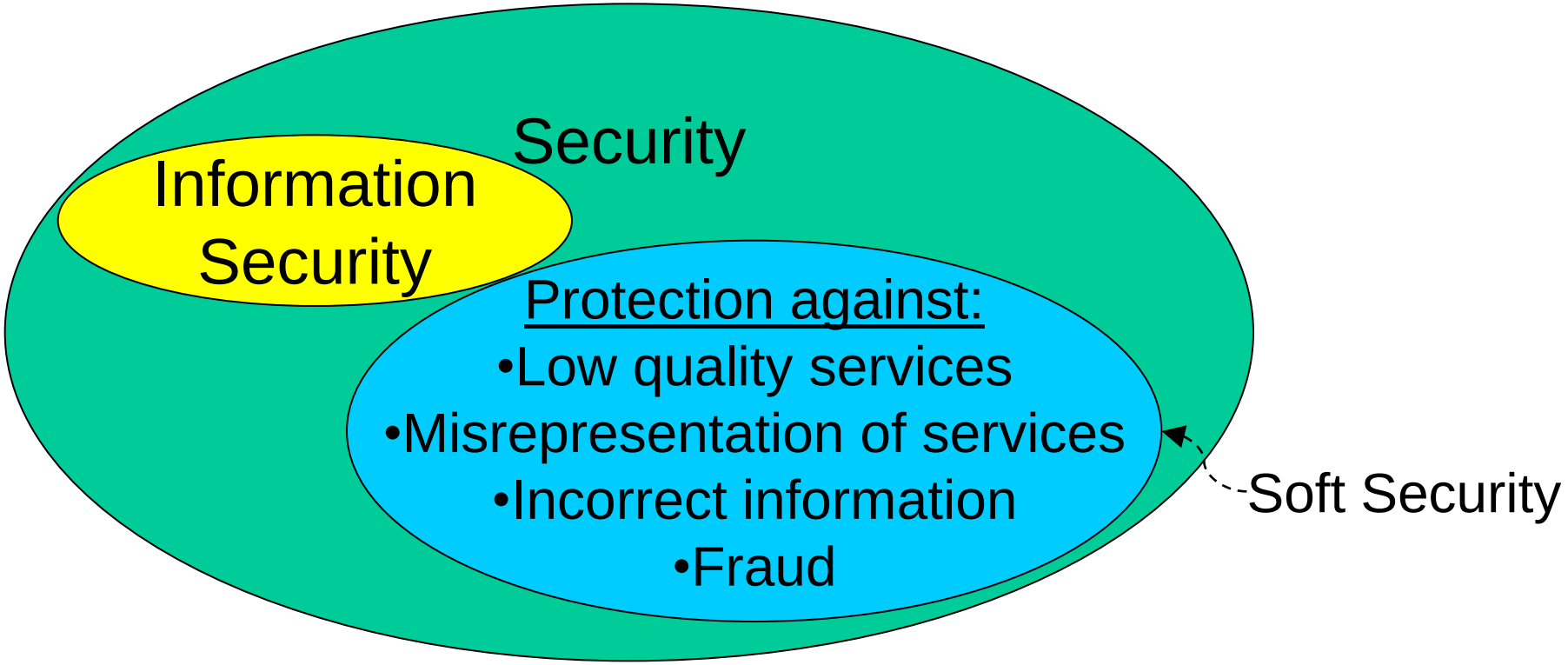
Car thieves chopped off part of the driver’s left index finger to start S-Class Mercedes Benz equipped with fingerprint key. Malaysia, March 2005 (NST picture by Mohd Said Samad)

Soft security and basic trust concepts

What is Security?

- General definition of security:
  - *Protection from danger*
  - Oxford English Online Dictionary: http://dictionary.oed.com/
- Traditional definition of information security:
  - *Preservation of confidentiality, integrity & availability of information*
  - ISO/IEC 27001:2005 Specification for an Information Security Management System
  - Assumes that the owner of information resources
    - defines a security policy (explicitly or implicitly)
    - implements measures to preserves CIA properties

Gap analysis of security and information security



Soft Security

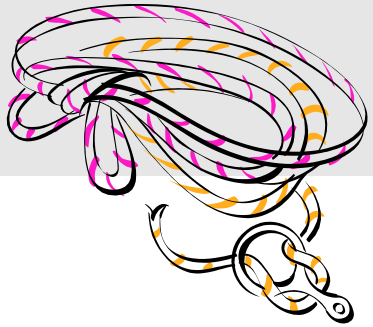
- Impossible to define security policies for open communities
- Common ethical norms instead of security policy
  - Can be partly formal and partly dynamic/collaborative
- Definition:
  - ***Adherence to common (ethical) norms***
- Stimulates the quality of communities in terms of ethical behaviour and integrity of its members
- Enforced by collaborative mechanisms such as trust and reputation systems

Two definitions of trust

- Evaluation trust
  - The **subjective probability** by which an individual, *A*, expects that another individual, *B*, performs a given action on which its welfare depends. (Gambetta 1988)

- Decision trust
  - The **willingness to depend** on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible. (McKnight & Chervany 1996)

Would you trust this rope?



For what?

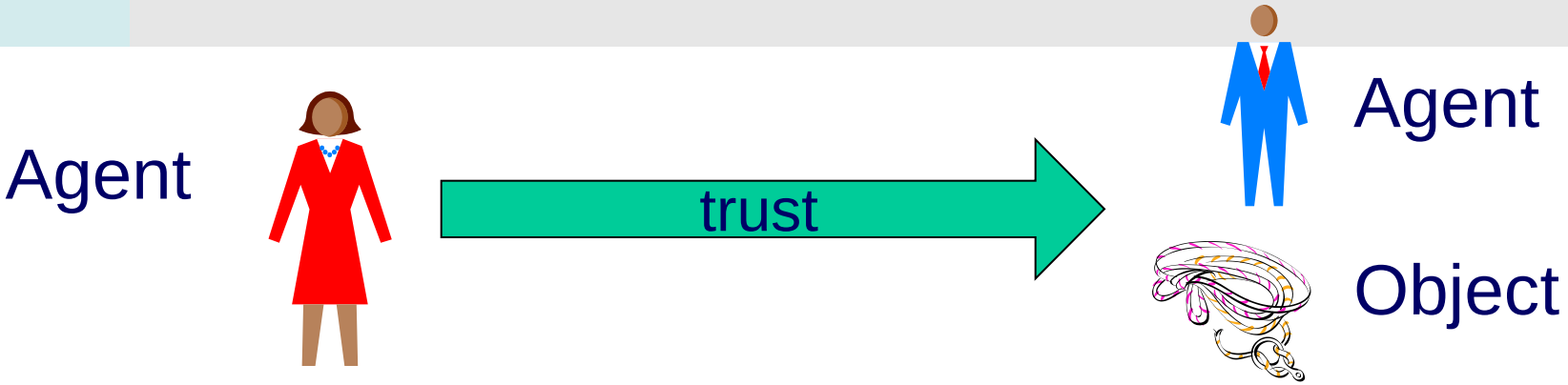
To climb down from the 3rd floor window of a house

The rope looks very old

Fire drill: **No!**

Real fire: **Yes!**

Trust is a relationship



- Trusting party
  - Also called
    - “relying party”
    - “trustor”
  - Is in a situation of
    - Dependence
- Trusted party
  - Also called
    - “trustee”
  - Is in a situation of
    - Power
    - Expectation to deliver

Two sides of trust management

Trusting party

Wants to **assess** and make **decisions** w.r.t. the dependability of the trusted party for a given transaction and context

Trusted party

Wants to **represent** and put in a **positive light** own competence, honesty, reliability and quality of service.

Reputation and trust

REPUTATION

- Public info
- Common opinion
- Not necessarily objective

TRUST

- Both private and public info
- Private info carries more weight
- Subjective

- *"I trust you because of your good reputation"*
- *"I trust you despite your bad reputation"*

Extrinsic and intrinsic trust

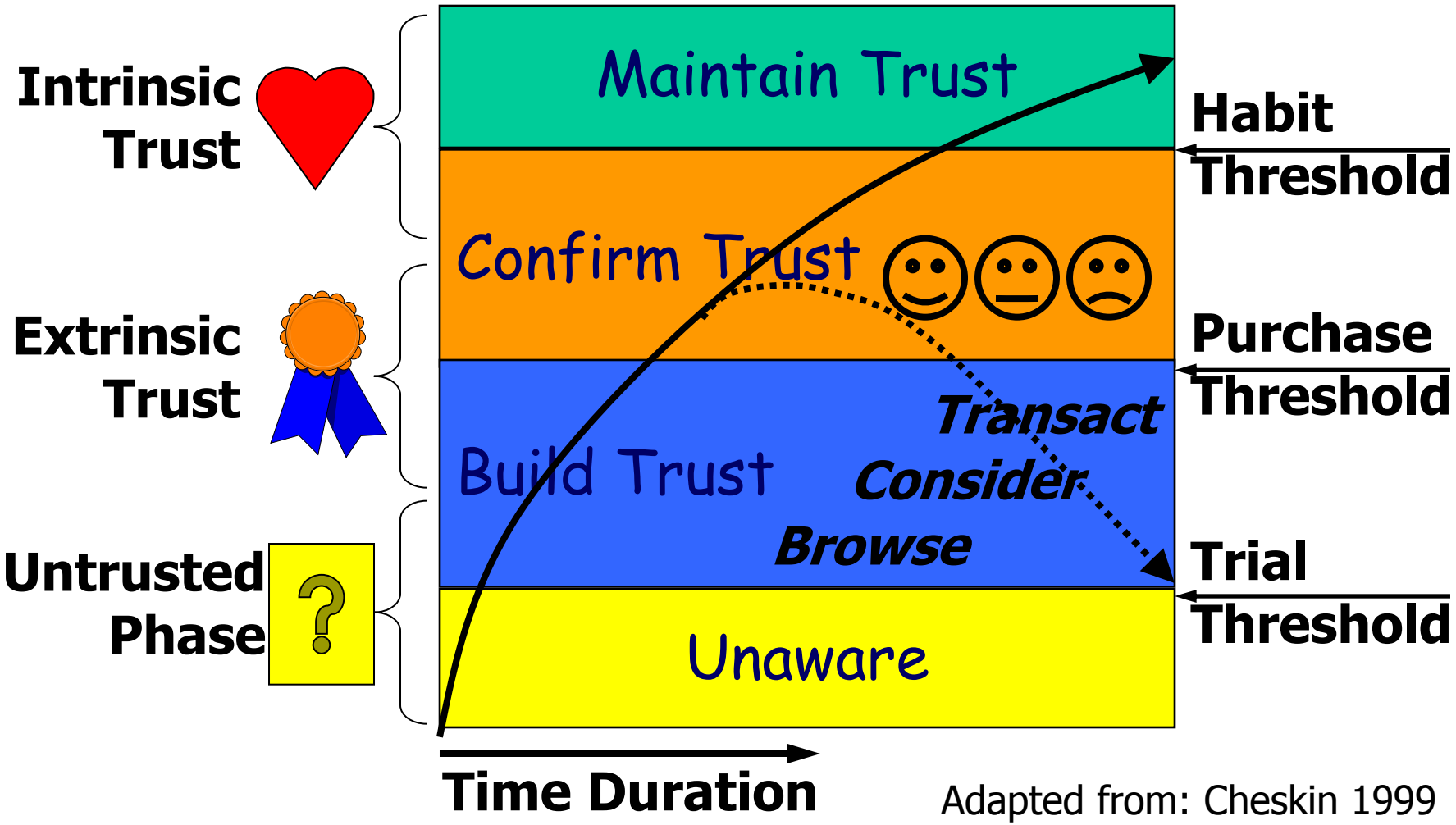
Extrinsic Factors

- Cognitive
- Observed
- Recommendation
- Reputation
- External evidence
- Easy to manufacture

Intrinsic Factors

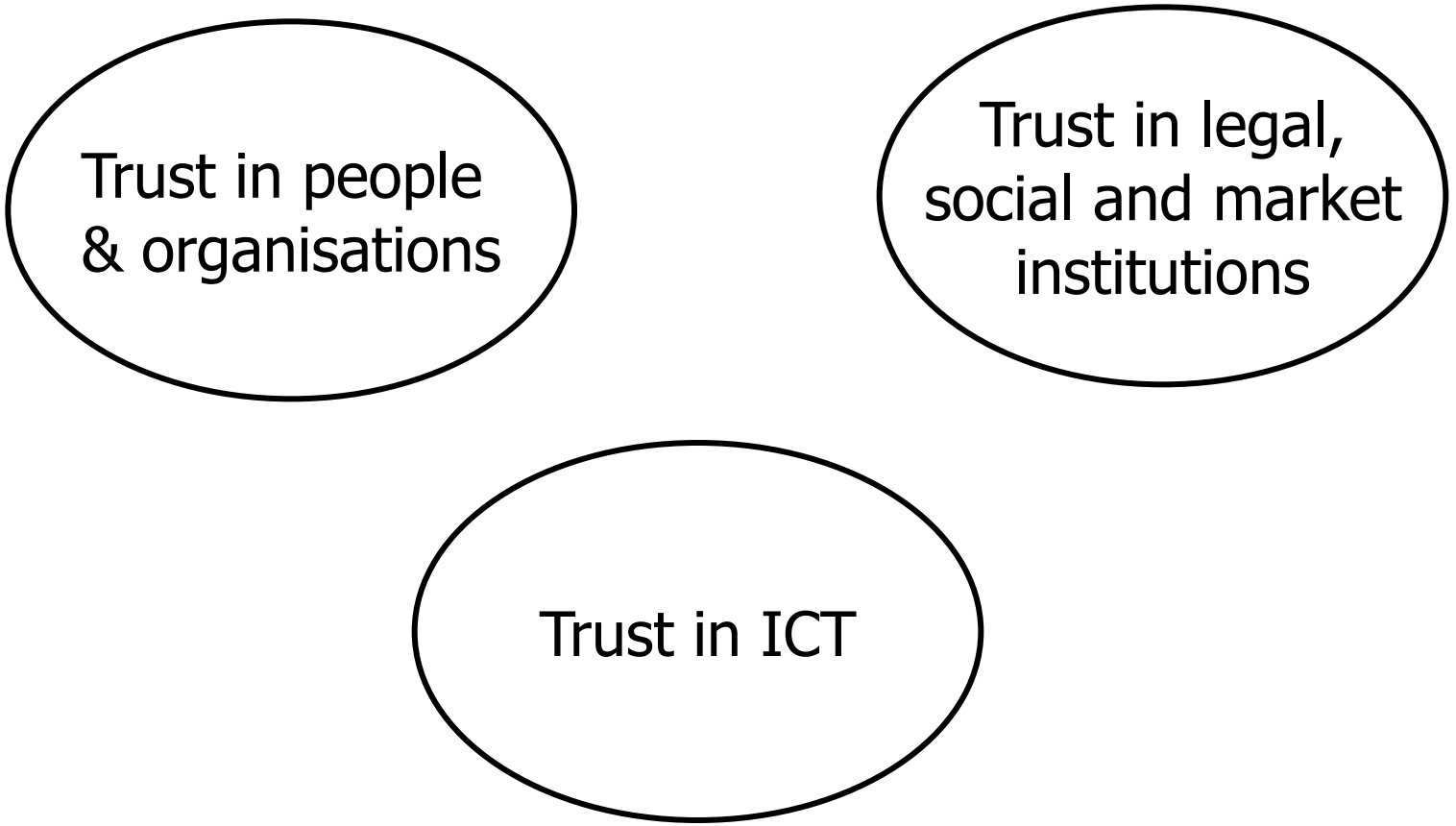
- Affective
- Experienced
- Intimate relationship
- Internalised pattern
- Take time to build
- Override extrinsic

A model for e-commerce trust



Adapted from: Cheskin 1999

We trust what we depend on



Why is the term “trust” so popular?

- Metaphorical trust expressions
  - IT security people like metaphors:
    - E.g. firewall, honeypot, virus, Trojan horse, digital signature
  - Trust expressions serve as simple metaphors for complex security concepts, e,g. , …, ***trusted code, circle of trust***, …
- Trust has very positive connotations
  - Trust expressions are ideal as marketing slogans

Trust expressions can be difficult to intuitively understand

Trust Expressions in IT security

Trust management

Trustworthy computing

Trusted code

Trust bar

Trust anchor

Trust ecology

Trusted Computing Base

Trust system

Trusted system

Trusted computing

Trusted Platform Module

Computational trust

Trust negotiation

Trust model

Trust provider

Circle of trust

Trusted Third Party

Trust metric

Evidence of an over-used concept

- The term “trust” can impossibly mean the same thing in all the different security expressions
- How do you know what it means?
- Be sceptical when someone uses the term trust
- Dieter Gollmann: Why Trust is Bad for Security

- End of talk
- Thank you for your attention