Making systems secure and usable – what can software developers do?

M. Angela Sasse
Professor of Human-Centred Technology
Director, Academic Centre of Excellence for Cyber Security Research & Research Institute for Science of Cyber Security
University College London, UK
www.ucl.cs.ac.uk/staff/A.Sasse

Background

Study on escalating cost of password resets at BT

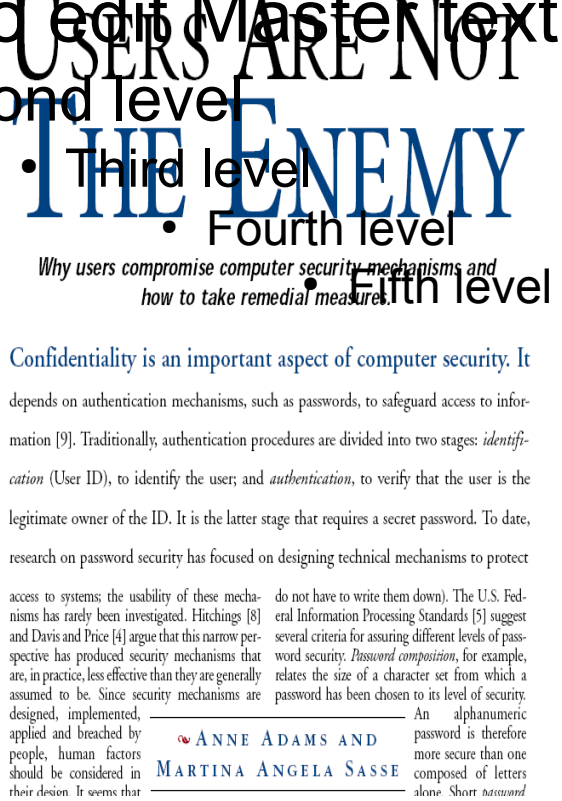
- too high workload
- leads to shortcut security mechanisms
- users don't understand threats and risks

Also 1999: Whitten & Tygar *"Why Johnny Can't Encrypt"*

Click to edit Master text styl

Second level

- Third level
- Fourth level
- Fifth level



USERS ARE NOT THE ENEMY

Why users compromise computer security mechanisms and how to take remedial measures.

Confidentiality is an important aspect of computer security. It depends on authentication mechanisms, such as passwords, to safeguard access to information [9]. Traditionally, authentication procedures are divided into two stages: *identification* (User ID), to identify the user; and *authentication*, to verify that the user is the legitimate owner of the ID. It is the latter stage that requires a secret password. To date, research on password security has focused on designing technical mechanisms to protect access to systems; the usability of these mechanisms has rarely been investigated. Hitchings [8] and Davis and Price [4] argue that this narrow perspective has produced security mechanisms that are, in practice, less effective than they are generally assumed to be. Since security mechanisms are designed, implemented, applied and breached by people, human factors should be considered in their design. It seems that

do not have to write them down). The U.S. Federal Information Processing Standards [5] suggest several criteria for assuring different levels of password security. *Password composition*, for example, relates the size of a character set from which a password has been chosen to its level of security. An alphanumeric password is therefore more secure than one composed of letters alone. Short *password*

ANNE ADAMS AND MARTINA ANGELA SASSE

Adams & Sasse CACM 1999

Progress since then?

ACM SOUPS (Symposium on Usable Security and Privacy) since 2004
SHB (Security & Human Behaviour) since 2008
Papers in CHI, CCS, Usenix, NSPW …
Books: Cranor & Garfinkel, Shostack, Lacey
University courses on usable security
US National Academy of Sciences Workshop on *Usable Security and Privacy* 2009

And – has it made security more usable? Consider authentication

Nielsen (2000) said that biometrics are highly usable and would replace passwords.
Schneier (2000) and Gates (2004) predicted that passwords would become obsolete
Hasn't happened – why not?
Research on usable security has produced many "better" authentication mechanisms – but we see little change in practice …

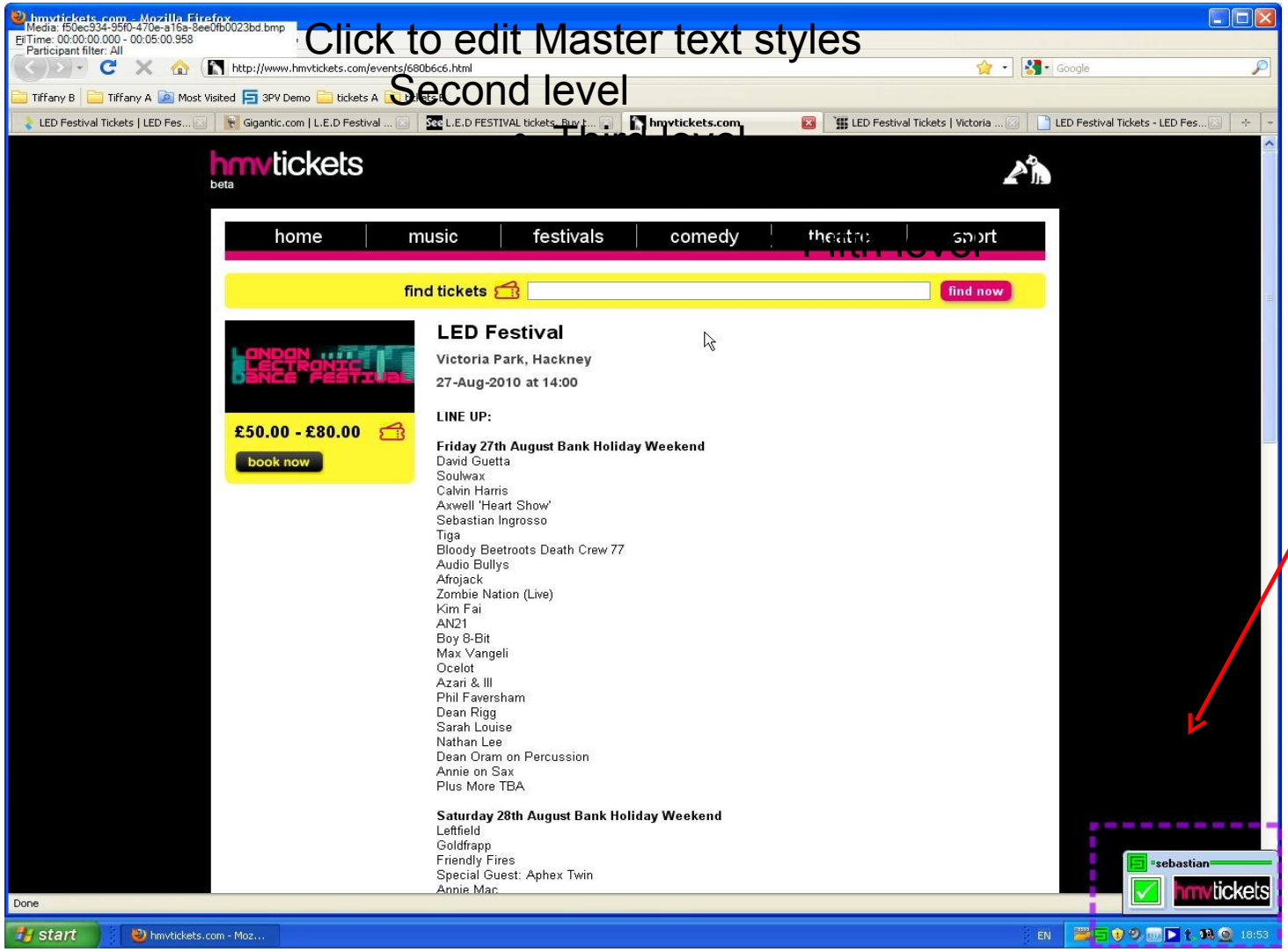
More ‘usable’ authentication ...

Authentication via Rorschach inkblot tests
Singing your password
Thinking your password (free EEG thrown in)
Schneier: fMRI would be cool
More biometrics (ear, nose, butt recognition)
Additional layers of knowledge-based credentials
Ringing up your friends in the middle of the night to provide you with previously entrusted re-set codes
Make people watch ads & authenticate by recognising 4 frames

Study 1 – Active anti-phishing tool

Passive phishing indicators do not work (Djamija et al., Wu et al.)
‘stop-look-listen’ for every web page?
Active anti-phishing tool: SOLID

SOLID Anti-phishing tool



Safe Website Green

Experimental design

- real-world *risk* in the experimental setup to produce ecologically valid results
- provide same incentives to users they see in real world

Website	Price	Potential reward	Condition	Actual reward
Gigantic	£50	£10	Real – Green	£10
HMV Tickets	£50	£10	Real – Green	£10
See	£25	£35	Fake – Red	£0
Skiddle	£20	£40	Real – Gray	£40
Sold-out ticket market	£40	£20	Fake – Gray	£0
View London	£20	£40	Fake - Yellow	£0

Did they look at the warning?

All participants looked at the tool window before making decision

Did they understand warning?

All participants said they understood what the different indicators signified
Interview data confirmed:

Green = safe

Red = unsafe

yellow = “something went wrong during authentication”

grey = unknown website.

Improvement in decision-making - BUT

significant difference in the participants' decisions when the tool was used compared to the control condition.
But: 8 in experimental condition still bought from grey & yellow sites …

Potential Payoff	Number of participants	
	Control	SOLID
£10	5	10 (green)
£35-40	12	8 (grey/yellow)
£20	1	0 (red)

Why do users ignore the tool?

Motivation: better price

Believe their own ability to judge a website is adequate to protect them against scams

- Past experience with high false-positive security tools creates a negative attitude

- Cormac Herley *(So Long, And No Thanks for All The Externalities*): users ignore security mechanism because they have high cost and little benefit

“Trust indicators” mentioned by participants

1. Previous experience with website
2. Logos and certifications
3. Advertisements
4. Social networking references
5. Inclusion of charity names
6. Amount of information provided
7. Website layout
8. Company information

Study 2 – Focus on one of the factors

Previous experience with website
Logos and certifications
Advertisements
Social networking references
Inclusion of charity names
Amount of information provided
Website layout
Company information

sse,
"Security education against phishing: A modest proposal for a major re-think",

Methodology

- 60 participants
- Six websites
- Two conditions

1) Original websites
2) Trust seals reversed (removed from sites that had one, added to those that didn't)

Click to edit Master text styles

Second level

- Third level
- Fourth level
- Fifth level

Click to edit Master text styles

Second level

- Third level
- Fourth level
- Fifth level

Were trust seals effective?

Eye-tracking data analysis results:

Only 12/60 participants noticed all three trust seals

23/60 did not notice any of them

No of seals noticed	No of participants
0	23
1	12
2	13
3	12

When noticed, trust seals influence ratings

Ratings assigned to websites			
Website	**Number of participants noticed**	**Rating when noticed**	**Rating when not noticed/not present**
eventim.co.uk	18	0.94	0.00
getmein.com	15	0.73	-0.04
gigantic.com	14	0.64	-0.11
hmvtickets.com	8	1.25	1.04
seetickets.com	11	0.27	0.37
skiddle.com	5	0.40	-0.40

- Statistically significant increase in ratings
  $t(5) = 3.3786$, $p = 0.0099$

But: is this influence a good thing?

participants made lots of assumptions

- Website is verified by the payment method company (e.g. VISA, MasterCard)
- Provides confirmation that website is genuine (could not explain why)

Conclusions - Trust seals don’t work

Not reliably noticed

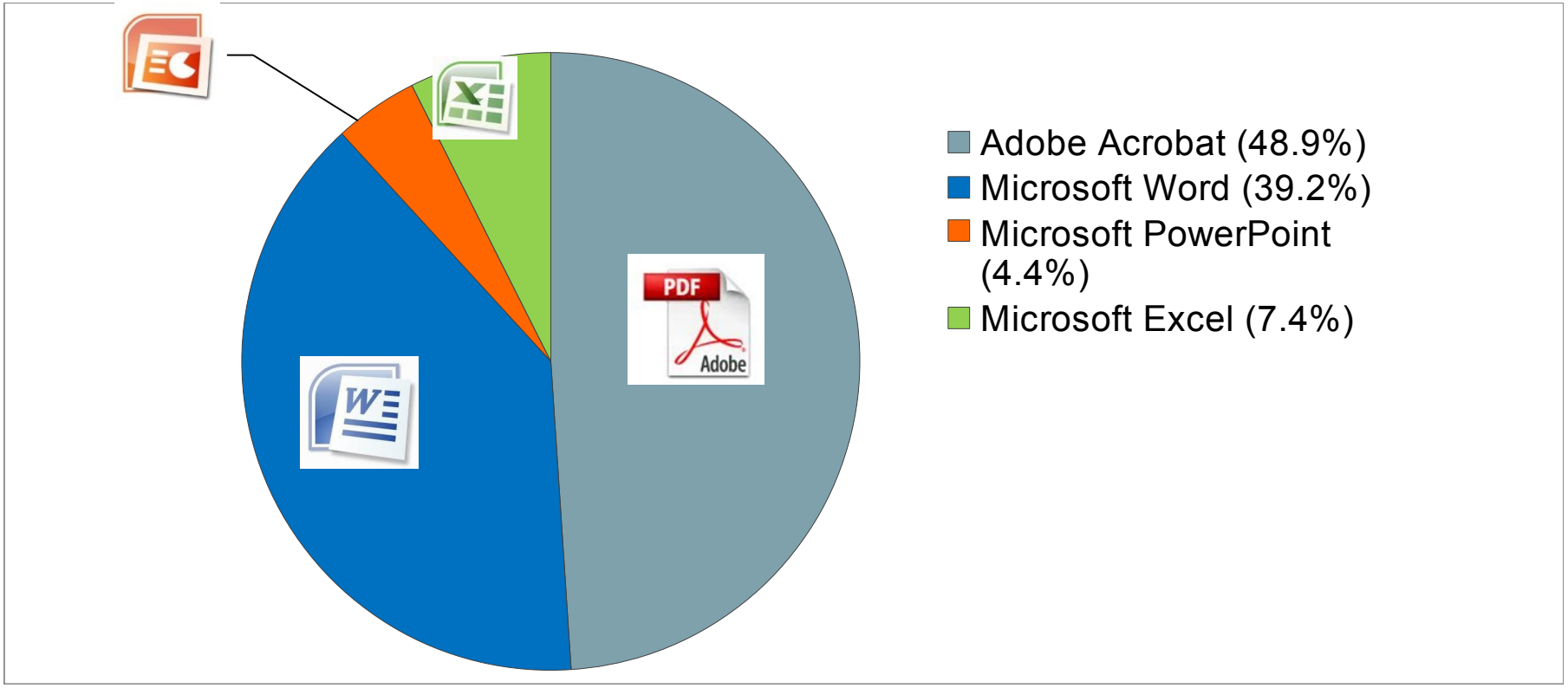
When noticed, they influence user perceptions towards trust, BUT people

- don’t verify them
- don’t understand what they mean
- attribute far too much protection

Makes most users more vulnerable!

Kirlappos, Sasse & Havey: Why Trust Seals Don’t Work. Procs TRUST2012

Study 3: pdf warnings

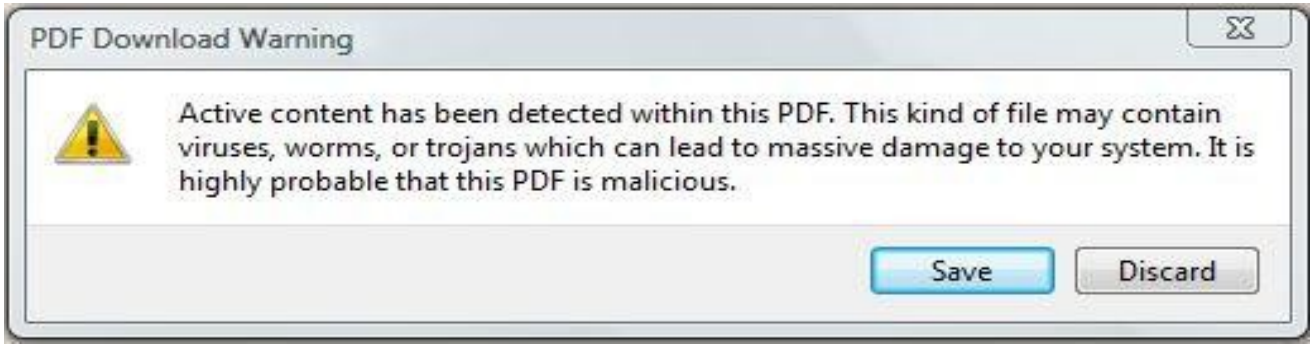


Most common file types in targeted attacks in 2009. Source: F-Secure (2010)

The experiment

Two conditions: between-subjects design

Participant
choos
choos
ants tried



General results

120 participants (64 female, mean age 25.7)

Warning type	Downloaded	Refused
Generic	52	8
Specific	46	14
∑	98	22

χ^2=1.391 p=0.238 df=1

Gender differences

	Download	Refusal
Male	50	6
Female	48	16
$\chi 2=4.071$, $p=0.044$, $df=1$		

Women were more cautious and less likely to download an article with a warning

Eye-tracking data

Fixation time in seconds

By warning type

- 6.13 for generic warnings
- 6.33 for specific warnings

By subsequent reaction

- 6.94 for those who subsequently refused to download
- 5.63 for those who subsequently downloaded the article

No significant difference between the length of fixation – all participants noticed the warning

Hypothetical vs. observed behaviour

Generic warning

	Download	Refusal to download
Hypothetical	52	8
Actual	41	19
	$\chi^2 = 6.039$, $p = 0.014$	

Specific warning

	Download	Refusal to download
Hypothetical	46	14
Actual	13	47
	$\chi^2 = 36.31$, $p < 0.0001$	

Conclusions: What can be done?

1. Kill all security tools with false positive rate higher than 1%.
2. Understand how much time and effort you are asking for
3. Security should not be an afterthought: Integrate security into task, eliminate choice, automatically direct users to safe option
4. Challenge dangerous misconceptions users have

Click to edit Master text styles

- Second level
- Third level
- Fourth level
- Fifth level

VeriSign Phish or No Phish?

VeriSign, Inc. (US) https://www.phish-no-phish.com

VeriSign

Which one is the phishing site?

3 of 10

THIS ONE

THIS ONE

Gordon Shopping.com - Microsoft Internet Explorer

https://www.gordonshopping.com/entercreditcard

GordonShopping.com

Discounts on leading brands

Checkout >> 1. Enter Your Address 2. Enter Your Card Infomation

Enter you're credit card inforemation below:

*Credit Card Type Visa

*Credit Card Number

*Card Security Code

*Expiration Date June 2011

Go

*Indicates a required field

Browse by Category

- Computers & Software
- Electronics
- PC Desktops
- Mac Desktops
- Monitors
- Tablet PCs
- Mice and Trackballs
- PDAs
- Printers
- Scanners

Bestsellers

Local intranet

Gordon Shopping.com - Microsoft Internet Explorer

https://www.gordonshopping.com/entercreditcard

GordonShopping.com

Discounts on leading brands

Checkout >> 1. Enter Your Address 2. Enter Your Card Information

Enter your credit card information below:

*Credit Card Type Visa

*Credit Card Number

*Card Security Code

*Expiration Date June 2011

Go

*Indicates a required field

Bestsellers

Local intranet

Better security education - Verisign ‘Phish or NoPhish’

Click to edit Master text styles

- Second level
- Third level
- Fourth level
- Fifth level

VeriSign Phish or No Phish?

VeriSign, Inc. (US) https://www.phish-no-phish.com

VeriSign

See why this is a fake site.

3 of 10

NEXT

Gordon Shopping.com - Microsoft Internet Explorer

https://www.gordonshopping.com/entercreditcard

GordonShopping.com

Discounts on leading brands

Checkout >> 1. Enter Your Address 2. Enter Your Card Information

Enter your credit card information below:

*Credit Card Type Visa

*Credit Card Number

*Card Security Code

*Expiration Date June 2011

Go

*Indicates a required field

Browse by Category

- Computers & Software
- Electronics
- PC Desktops
- Mac Desktops
- Monitors
- Tablet PCs
- Mice and Trackballs
- PDAs
- Printers
- Scanners

Bestsellers

Often, phishing sites will look just like the real thing. However, if you look closely, you may spot misspellings and other typos that indicate the site is fraudulent. Misspellings may also appear in the preliminary email, too.

Obstacle security = bad security

Encourages workarounds …

Security that supports user goals

Give an Allowance with Amazon PayPhrase

What is Amazon PayPhrase?

PayPhrase is an easy-to-remember shortcut to the payment and shipping information in your Amazon.com account. Each PayPhrase can be configured with simple controls, including monthly spending limits and e-mail alerts, so you can share your account with family members without sharing your credit card number or account password.

PayPhrase allowance controls include:

- Monthly spending limits
- Unspent allowance roll-over settings
- Order approval by e-mail or text message

› Create your PayPhrase

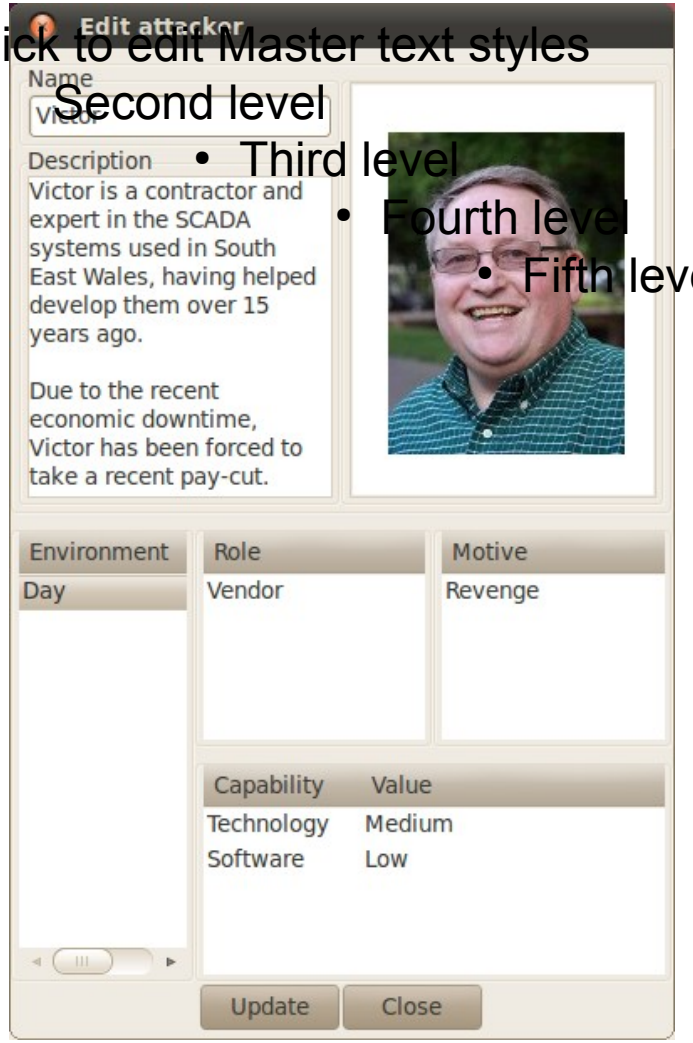
Integrate requirements into specs

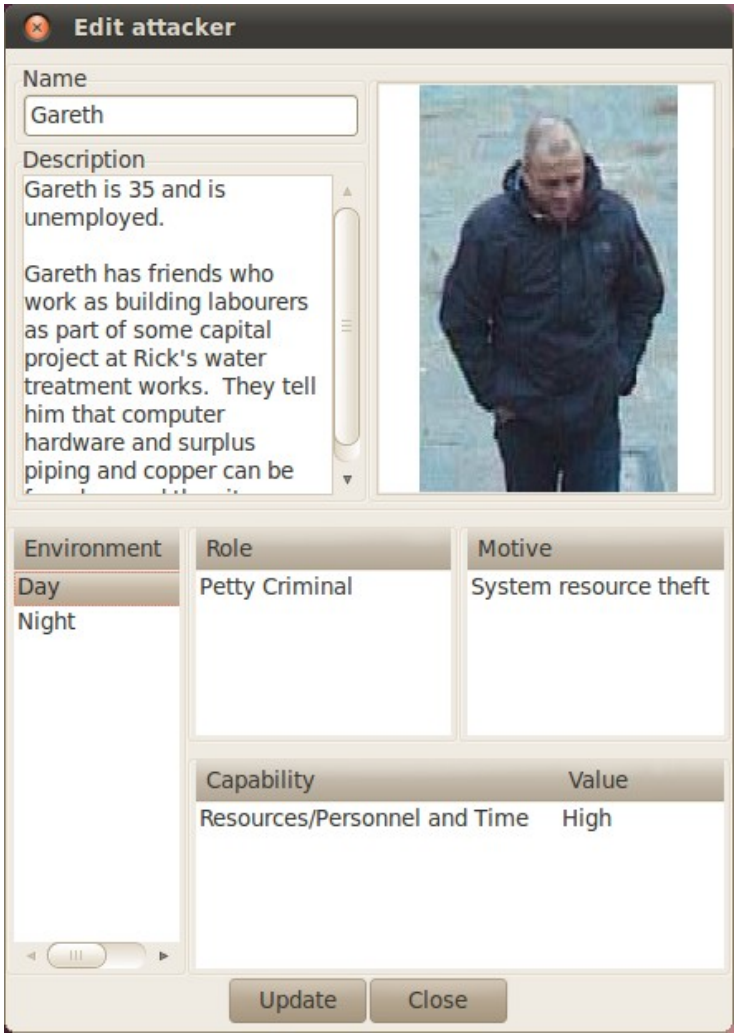
AEGIS – Integration of security and usability into requirements process, UML (Fléchais, Sasse & Mascolo, 2007)
IRIS – meta-model, based on KAOS (Faily & Fléchais, 2010)
Integration of personas (Faily & Fléchais, 2010)
CAIRIS – software tool to support process (Faily & Flechais 2011)

Personas for attackers

Click to edit Master text styles

- Second level
- Third level
- Fourth level
- Fifth level





Back to good old 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 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.**

Auguste Kerckhoffs, 'La cryptographie militaire',
Journal des sciences militaires, vol. IX, pp. 5–38, Jan. 1883, pp. 161–191, Feb. 1883.