The Use of Smartphone in the Chain of Security

When all Becomes Electronically ---except the User

Who Berne University of Applied Sciences (BFH)
Research Institute for Security in the Information Society (RISIS)
E-Voting Group
Eric Dubuis, Rolf Haenni, Reto E. Koenig
IoT Group
Andreas Danuser, Franz Meyer, Reto E. Koenig

Why Experts in Remote Voting Over the Internet (E-Voting)
Demonstration of Voulnerabilities in E-Banking Systems (2012)
Demonstration of Voulnerabilities in E-Voting System (2013)
Demonstration of Voulnerability in E-Banking Solution (2014)

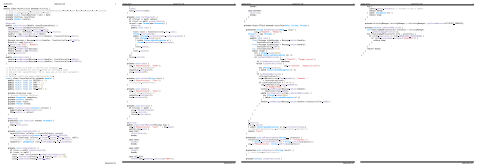
Quest Stop using Smartphones as Part of the Security Chain
Start using Secure Hardware Tokens instead

Berner Fachhochschule

What is It All About?

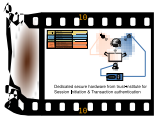
"This client option provides a secure cost-effective mobile tool for strong transaction authentication anywhere, anytime, without the need of an extra device."

Demo Transaction Substitution Exploit On a Current **Secure** E-Banking Solution



History of E-Banking and Security: From Past to Future

Introduction of Smartphone
Into the Chain of Security



Introduction of a Dedicated *Secure Hardware Token**
Into the Chain of Security

* Provided by Trustworthy Site
Secure Channel to Trusted Site
Non Reprogrammable
Secure Keyboard
Secure Display

How to Infect *General Purpose Device**

* Uncontrolled Provider
Connected to the Internet
Freely Reprogrammable

An Infected Browser is All It Needs

How Infected Devices Communicate

There is no Air Gap

The Use of Smartphone in the Chain of Security

When all Becomes Electronically ---except the User

Who Berne University of Applied Sciences (BFH)
Research Institute for Security in the Information Society (RISIS)
E-Voting Group
Eric Dubuis, Rolf Haenni, Reto E. Koenig
IoT Group
Andreas Danuser, Franz Meyer, Reto E. Koenig

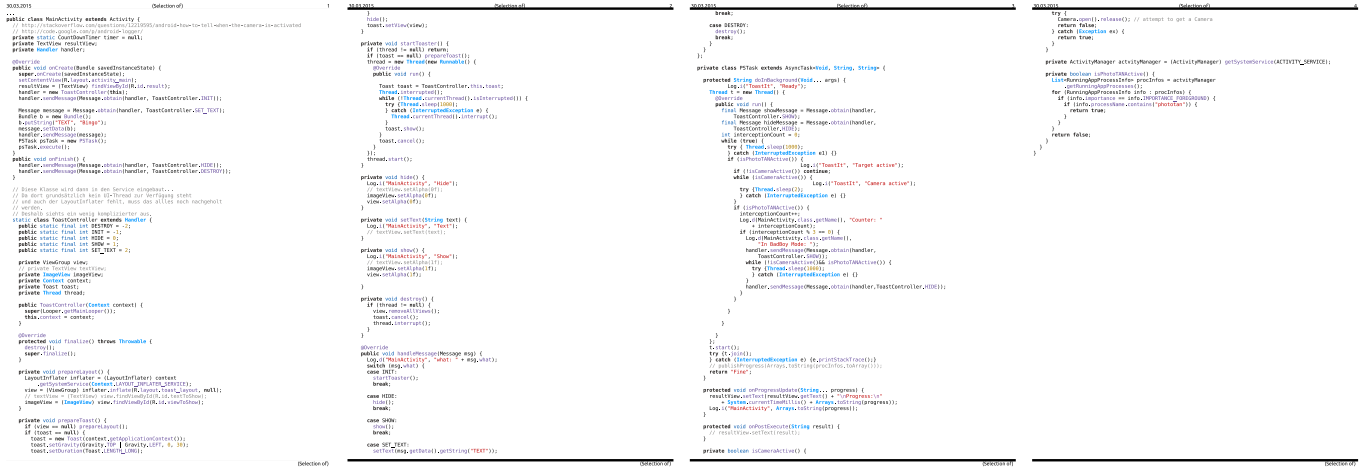
Why Experts in Remote Voting Over the Internet (E-Voting)
Demonstration of Voulnerabilities in E-Banking Systems (2012)
Demonstration of Voulnerabilities in E-Voting System (2013)
Demonstration of Voulnerability in E-Banking Solution (2014)

Quest Stop using Smartphones as Part of the Security Chain
Start using Secure Hardware Tokens instead

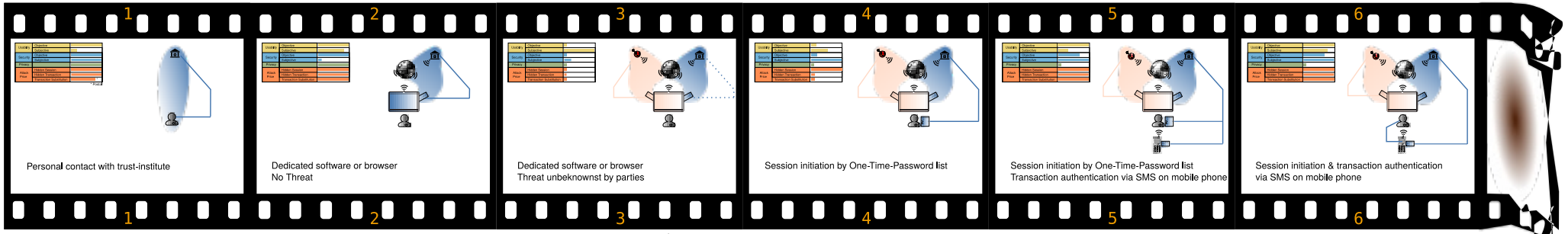
What is It All About?

"This client option provides a secure cost-effective mobile tool for strong transaction authentication anywhere, anytime, without the need of an extra device."

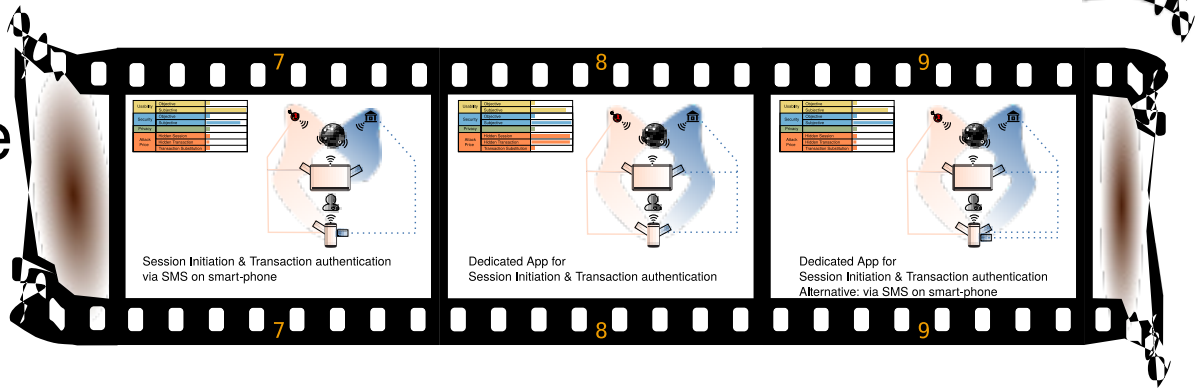
Demo Transaction Substitution Exploit On a Current **Secure** E-Banking Solution

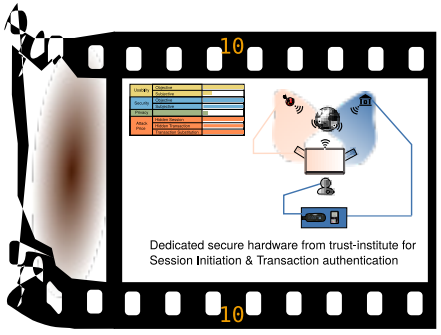


History of E-Banking and Security: From Past to Future



Introduction of Smartphone Into the Chain of Security



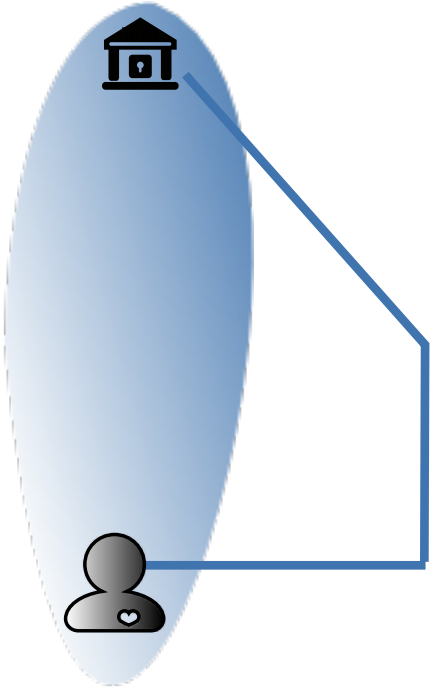


Introduction of a Dedicated *Secure Hardware Token** Into the Chain of Security

* Provided by Trustworthy Site
Secure Channel to Trusted Site
Non Reprogrammable
Secure Keyboard
Secure Display

Usability	Objective	
	Subjective	
Security	Objective	
	Subjective	
Privacy		
Attack Price	Hidden Session	
	Hidden Transaction	
	Transaction Substitution	*

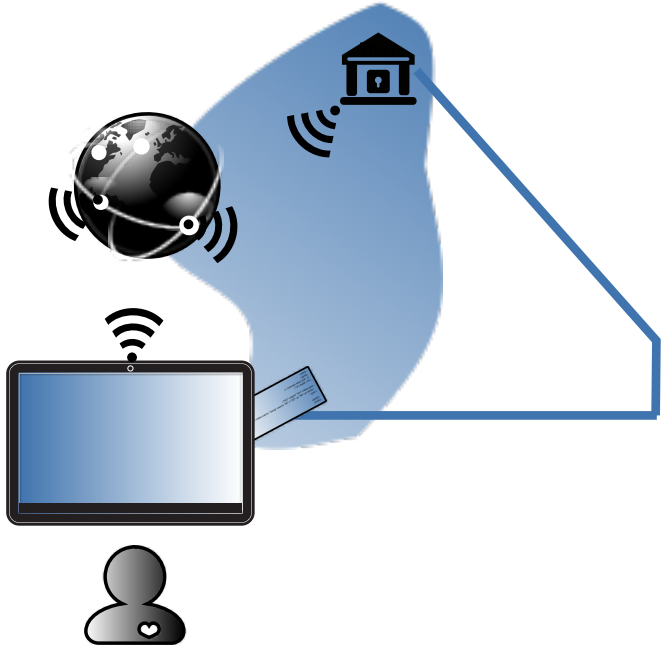
* Postal



Personal contact with trust-institute

2

Usability	Objective	
	Subjective	
Security	Objective	
	Subjective	
Privacy		
Attack Price	Hidden Session	
	Hidden Transaction	
	Transaction Substitution	

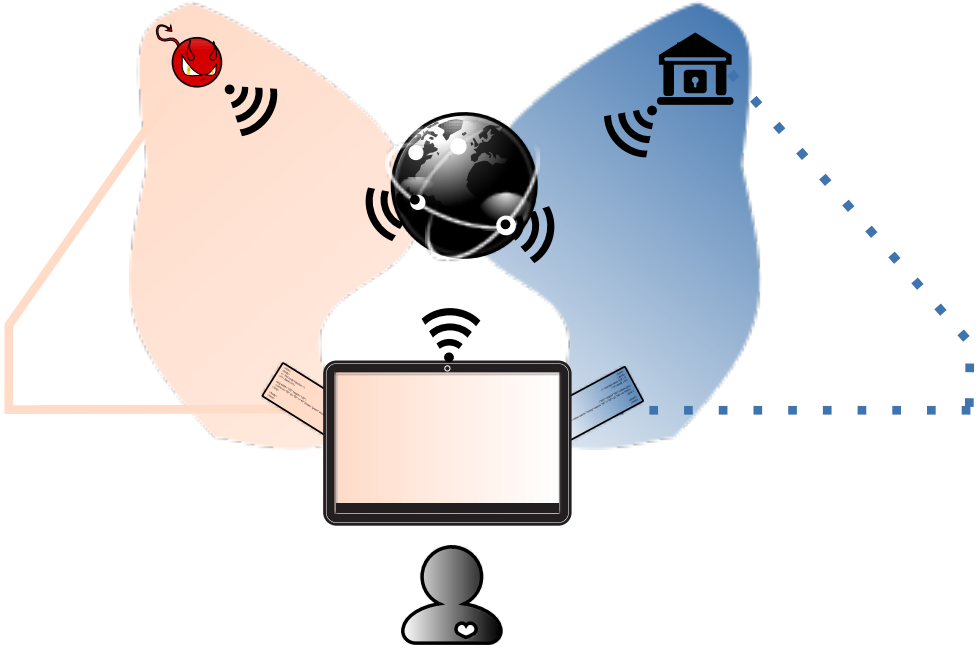


Dedicated software or browser

No Threat

3

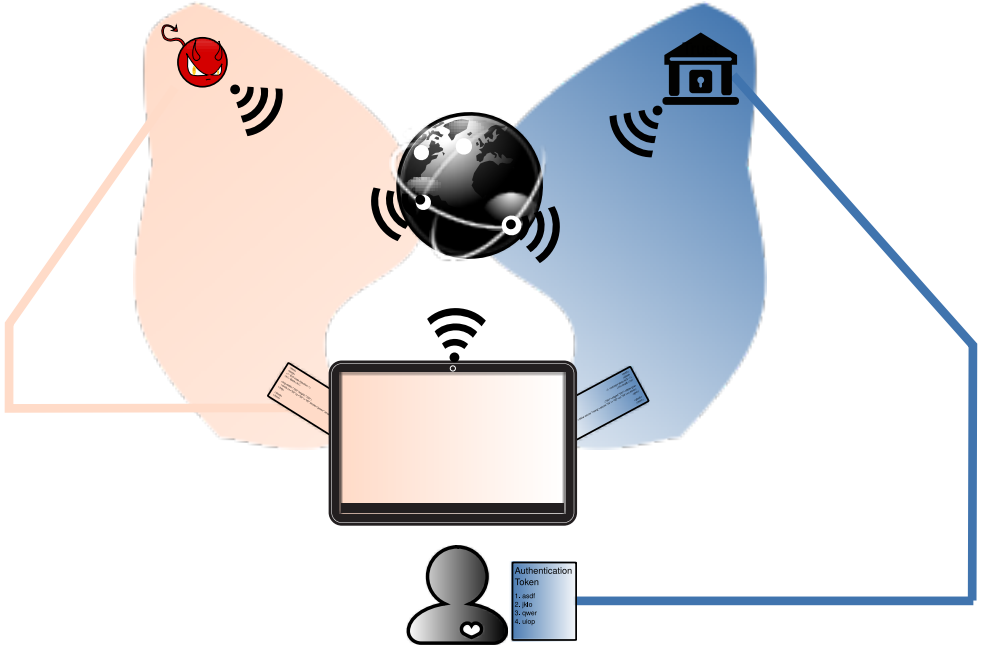
Usability	Objective	
	Subjective	
Security	Objective	
	Subjective	
Privacy		
Attack Price	Hidden Session	
	Hidden Transaction	
	Transaction Substitution	



Dedicated software or browser
Threat unbeknownst by parties

4

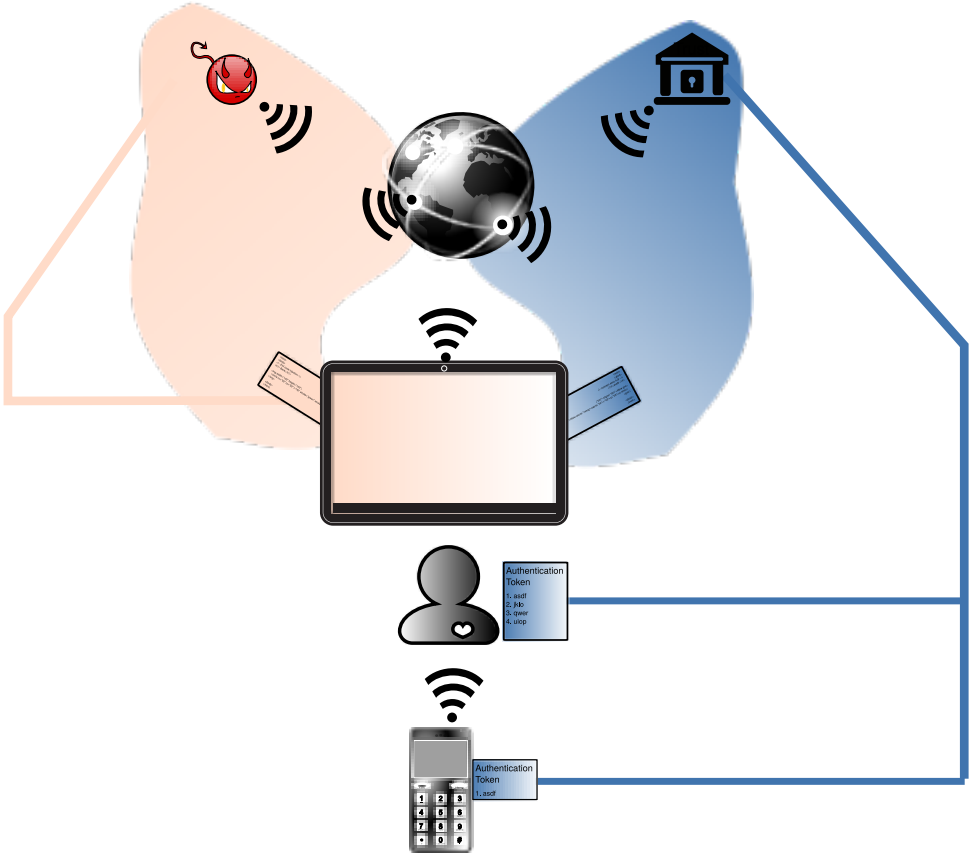
Usability	Objective	
	Subjective	
Security	Objective	
	Subjective	
Privacy		
Attack Price	Hidden Session	
	Hidden Transaction	
	Transaction Substitution	



Session initiation by One-Time-Password list

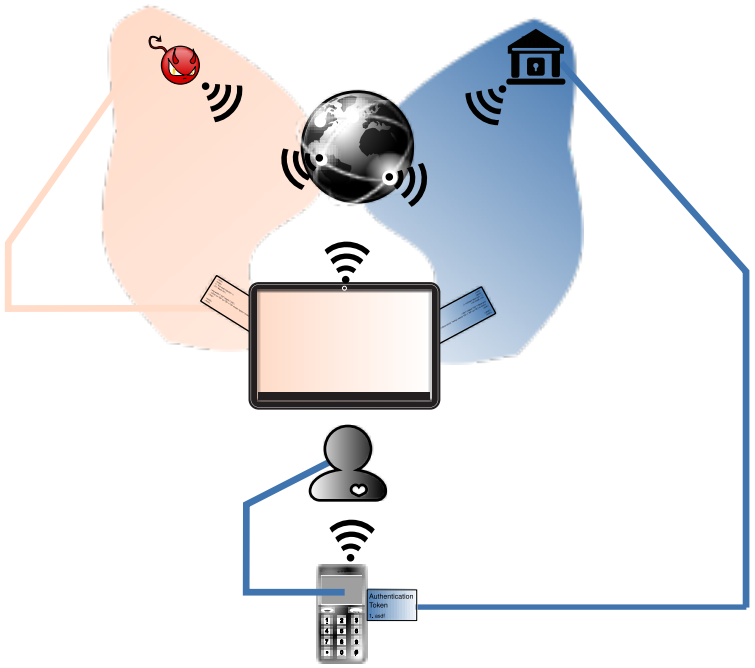
5

Usability	Objective	
	Subjective	
Security	Objective	
	Subjective	
Privacy		
Attack Price	Hidden Session	
	Hidden Transaction	
	Transaction Substitution	



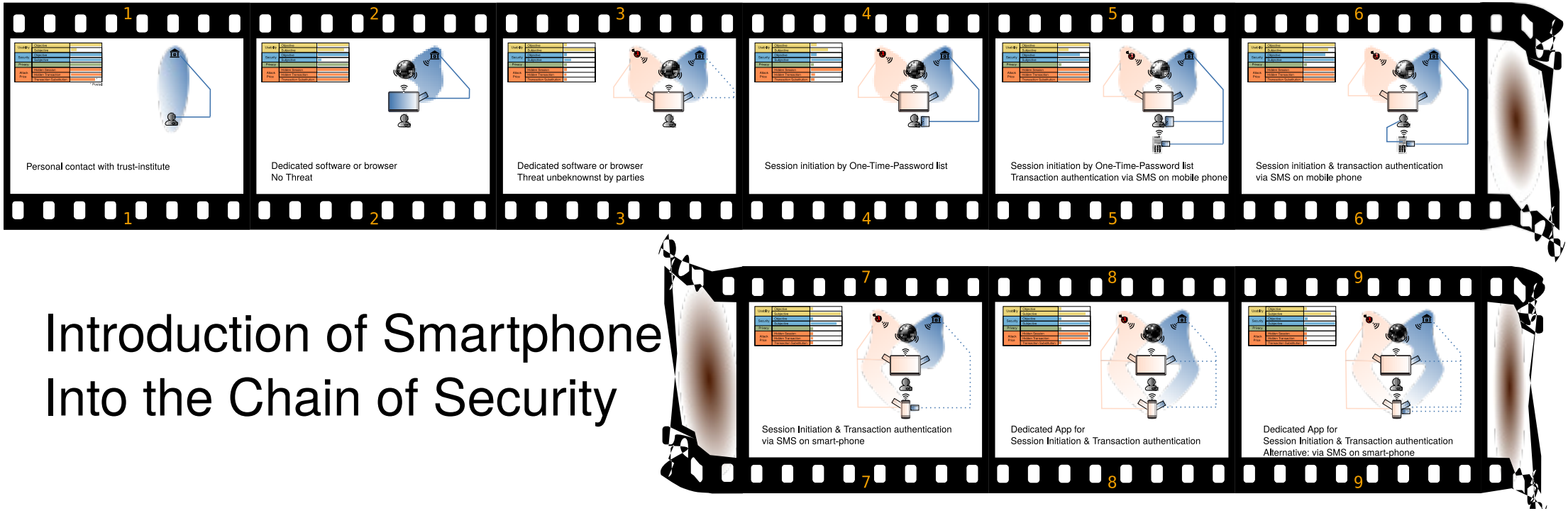
Session initiation by One-Time-Password list
Transaction authentication via SMS on mobile phone

Usability	Objective	
	Subjective	
Security	Objective	
	Subjective	
Privacy		
Attack Price	Hidden Session	
	Hidden Transaction	
	Transaction Substitution	

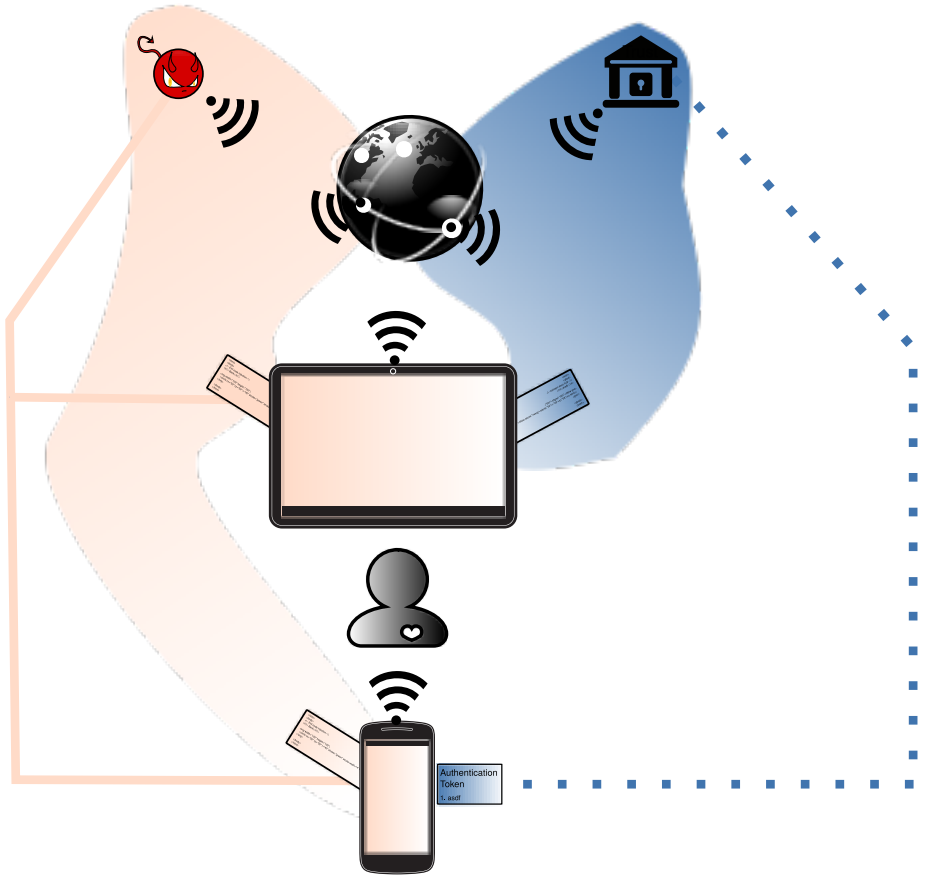


Session initiation & transaction authentication via SMS on mobile phone

Introduction of Smartphone Into the Chain of Security



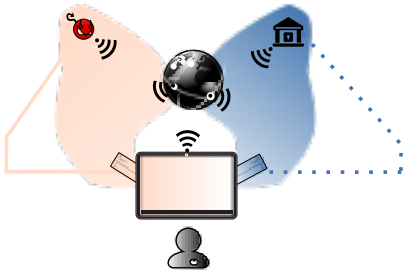
Usability	Objective	
	Subjective	
Security	Objective	
	Subjective	
Privacy		
Attack Price	Hidden Session	
	Hidden Transaction	
	Transaction Substitution	



Session Initiation & Transaction authentication via SMS on smart-phone

3

Usability	Objective	
	Subjective	
Security	Objective	
	Subjective	
Privacy		
Attack Price	Hidden Session	
	Hidden Transaction	
	Transaction Substitution	

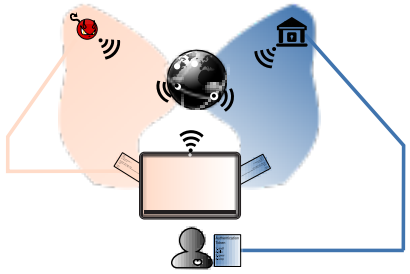


Dedicated software or browser
Threat unbeknownst by parties

3

4

Usability	Objective	
	Subjective	
Security	Objective	
	Subjective	
Privacy		
Attack Price	Hidden Session	
	Hidden Transaction	
	Transaction Substitution	



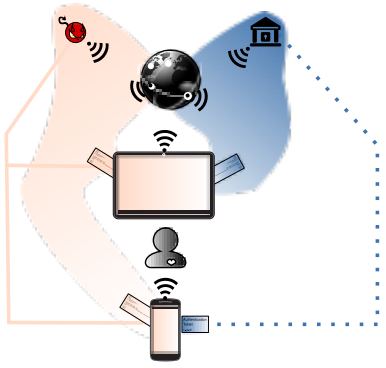
Session initiation by One-Time-Password list

4

ırtphone
ecurity

7

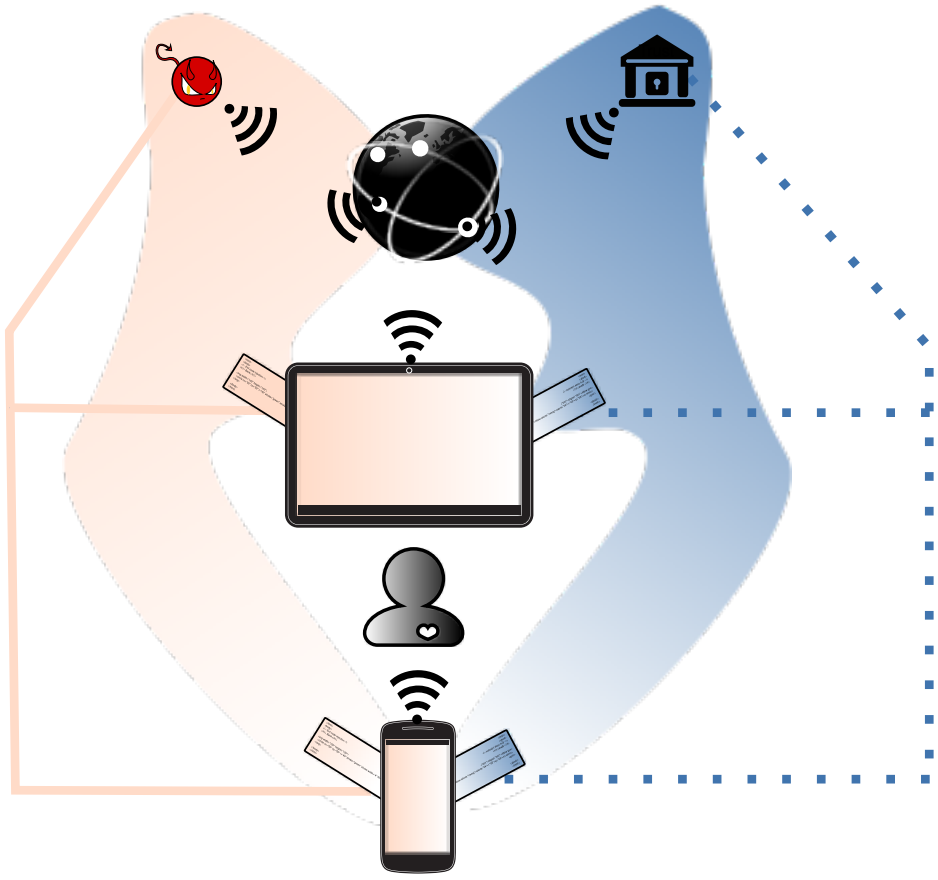
Usability	Objective	
	Subjective	
Security	Objective	
	Subjective	
Privacy		
Attack Price	Hidden Session	
	Hidden Transaction	
	Transaction Substitution	



Session Initiation & Transaction authentication
via SMS on smart-phone

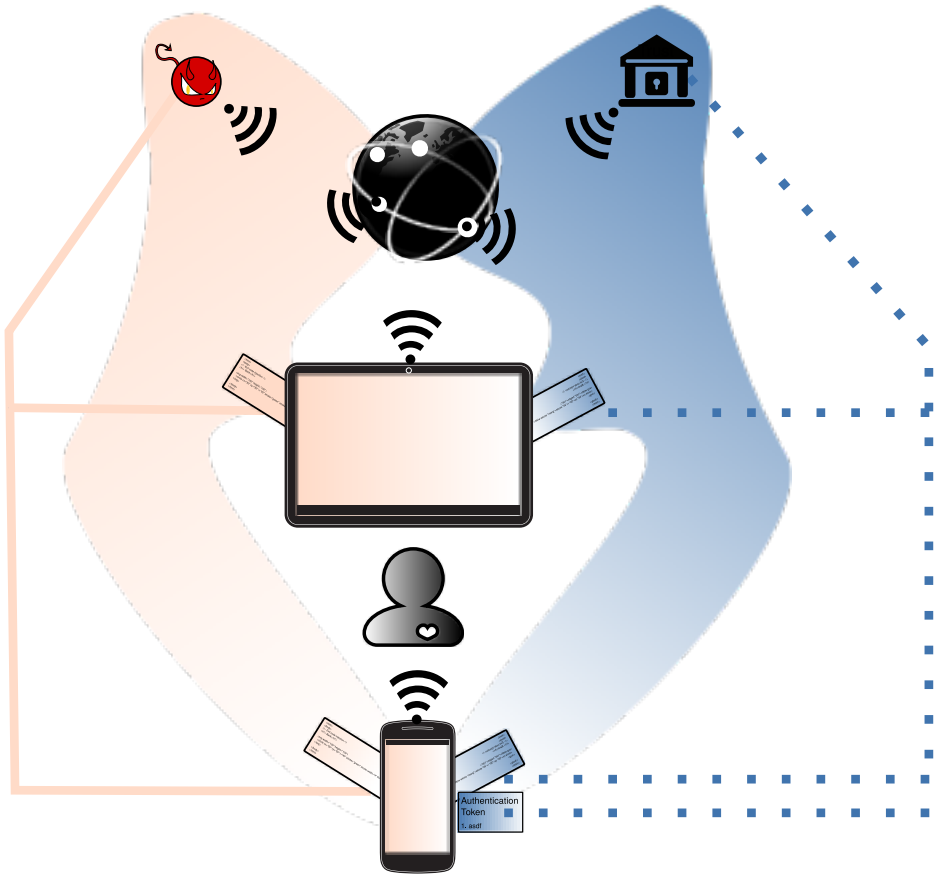
8

Usability	Objective	
	Subjective	
Security	Objective	
	Subjective	
Privacy		
Attack Price	Hidden Session	
	Hidden Transaction	
	Transaction Substitution	

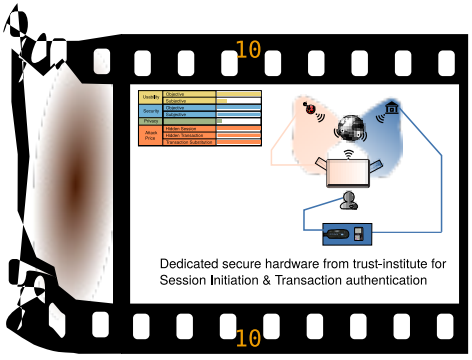


Dedicated App for
Session Initiation & Transaction authentication

Usability	Objective	
	Subjective	
Security	Objective	
	Subjective	
Privacy		
Attack Price	Hidden Session	
	Hidden Transaction	
	Transaction Substitution	



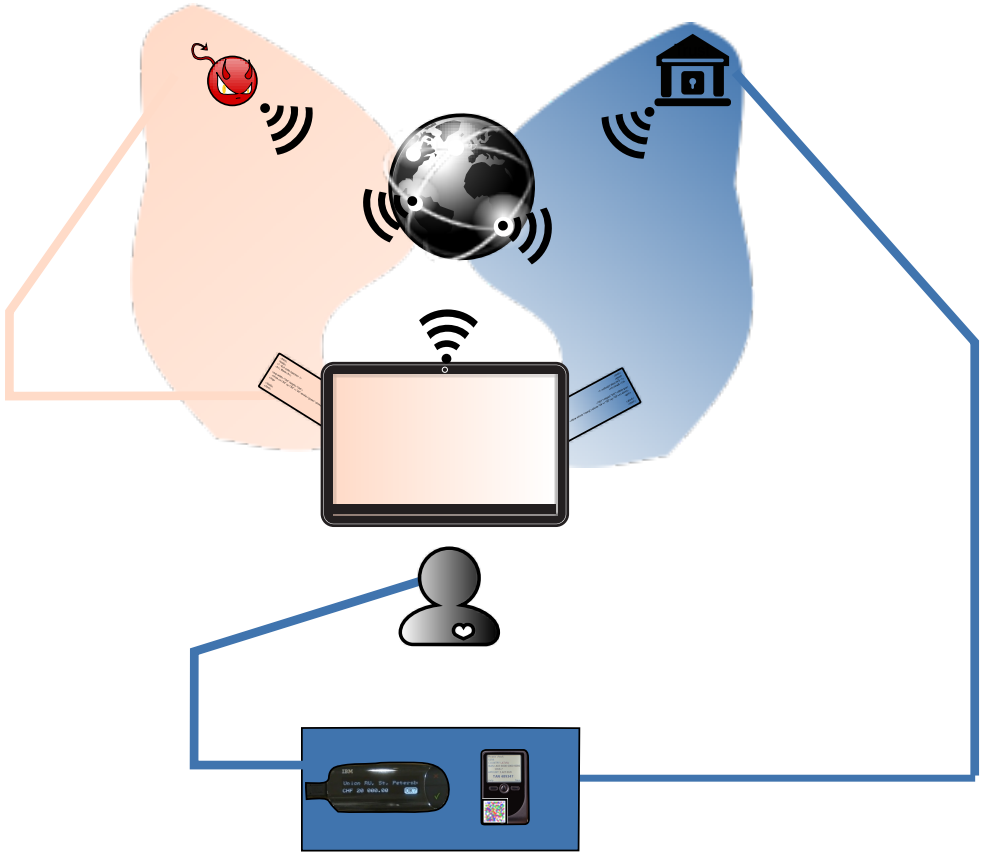
Dedicated App for
Session Initiation & Transaction authentication
Alternative: via SMS on smart-phone



Introduction of a Dedicated *Secure Hardware Token** Into the Chain of Security

* Provided by Trustworthy Site
Secure Channel to Trusted Site
Non Reprogrammable
Secure Keyboard
Secure Display

Usability	Objective	
	Subjective	
Security	Objective	
	Subjective	
Privacy		
Attack Price	Hidden Session	
	Hidden Transaction	
	Transaction Substitution	



Dedicated secure hardware from trust-institute for Session Initiation & Transaction authentication

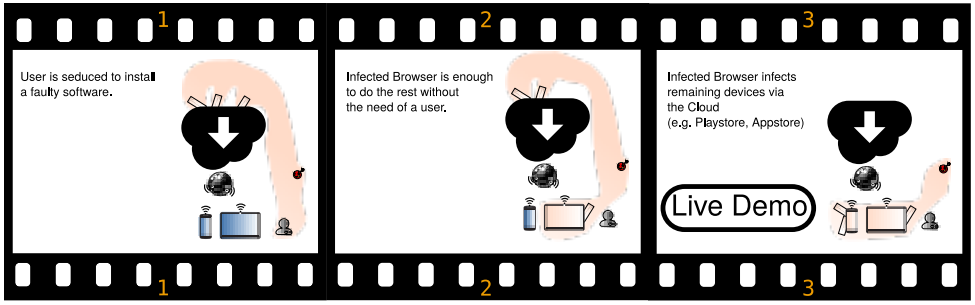
*Secure Hardware Token**

* Provided by Trustworthy Site
Secure Channel to Trusted Site
Non Reprogrammable
Secure Keyboard
Secure Display

How to Infect *General Purpose Device**

* Uncontrolled Provider
Connected to the Internet
Freely Reprogrammable

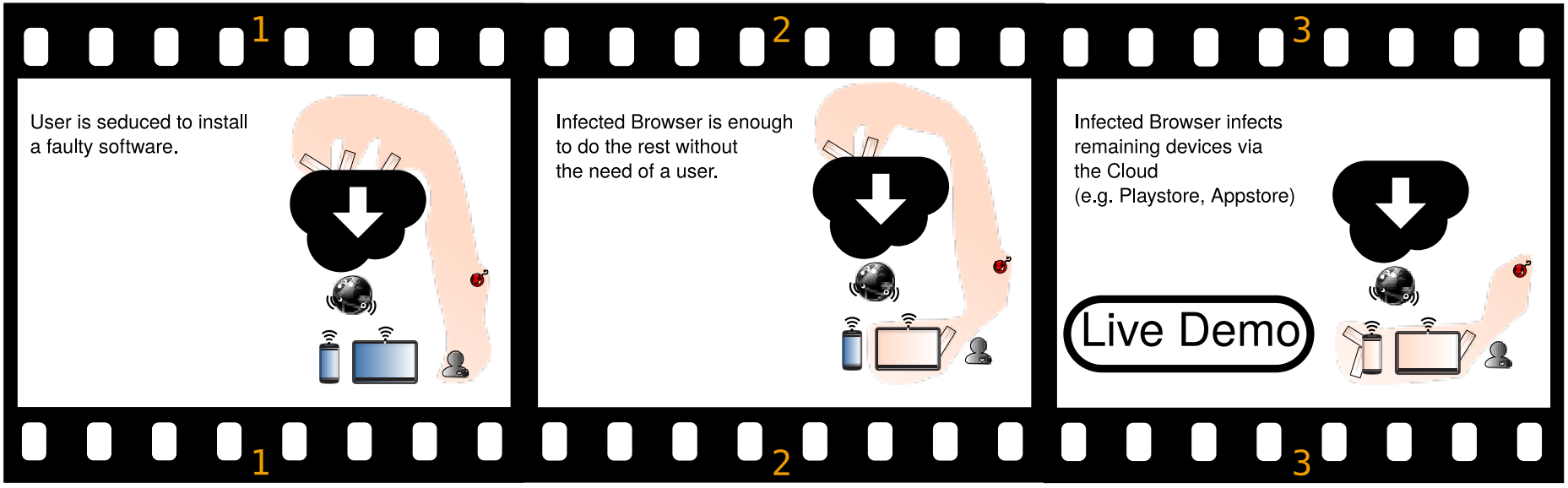
An Infected Browser is All It Needs



General Purpose Device*

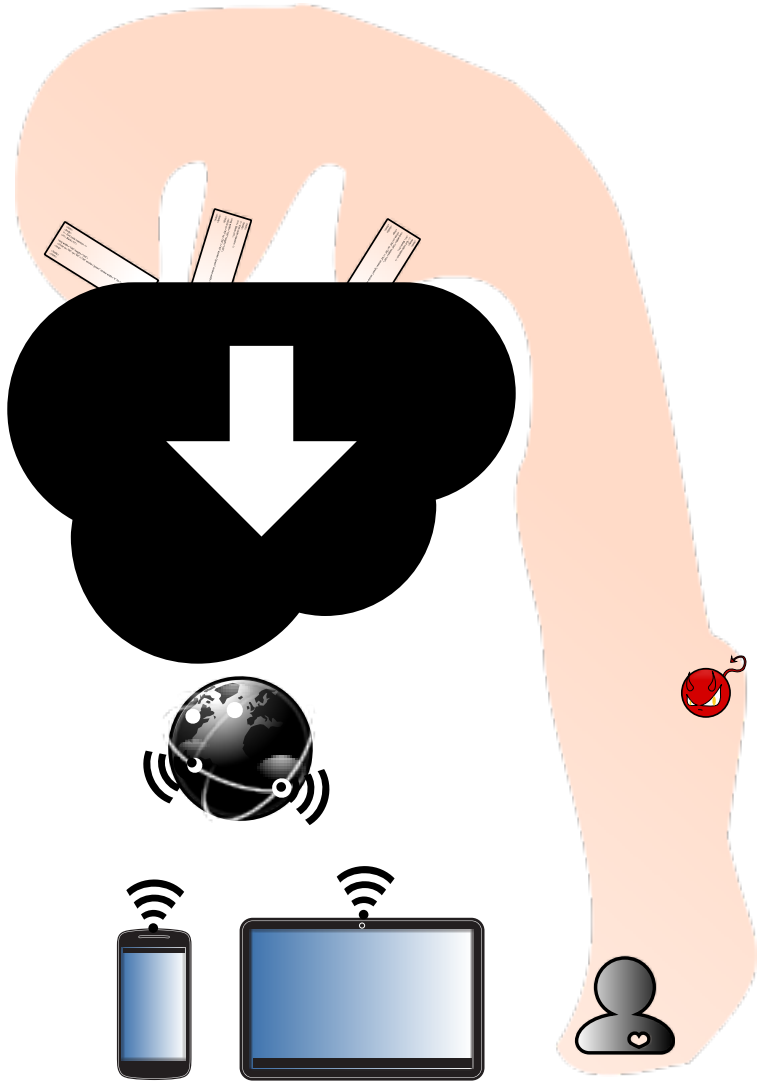
* Uncontrolled Provider
Connected to the Internet
Freely Reprogrammable

An Infected Browser is All It Needs



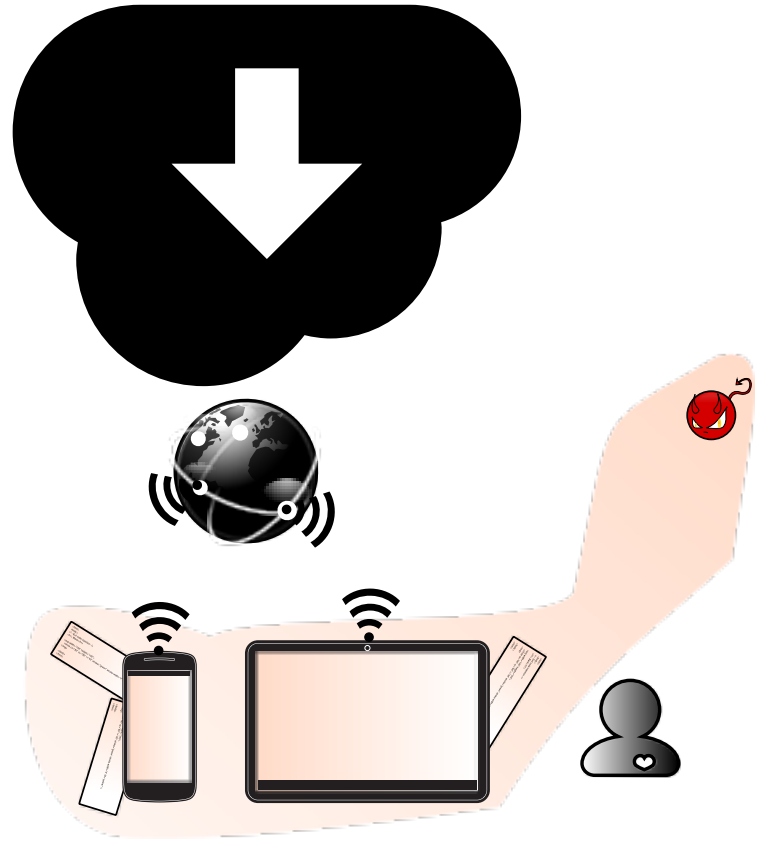
1

User is seduced to install a faulty software.



3

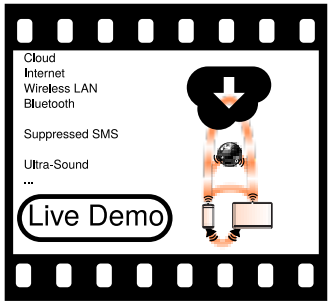
Infected Browser infects
remaining devices via
the Cloud
(e.g. Playstore, Appstore)



Live Demo

How Infected Devices Communicate

There is no Air Gap



There is no Air Gap