Threats and risks to mobile phones in Japan

Symantec Security Response

Kaoru Hayashi

Agenda

- Market and Technologies
- Current Threats
- Future Threats
- Success Factors
- Appendix

Market

	Carrier	Subscribers	Browser Phone Subscribers
Mobile Phone	NTT DoCoMo	49,779,300	45,003,400
	au	20,538,600	19,157,700
	Vodafone	14,988,200	12,786,400
	TuKa	3,526,200	
PHS	WillCom	3,366,900	
	NTT DoCoMo	1,040,800	
	ASTEL	74,900	
Total		93,314,900	76,947,500

73%

60%

Total Population in Japan:127,620,000

I'm going to speak about….

- FOMA
  - NTT DoCoMo's 3G mobile phones
  - 15,878,300 subscribers

- Except for M1000 model
  - This is quite different from other FOMA phones
  - Picking this up later

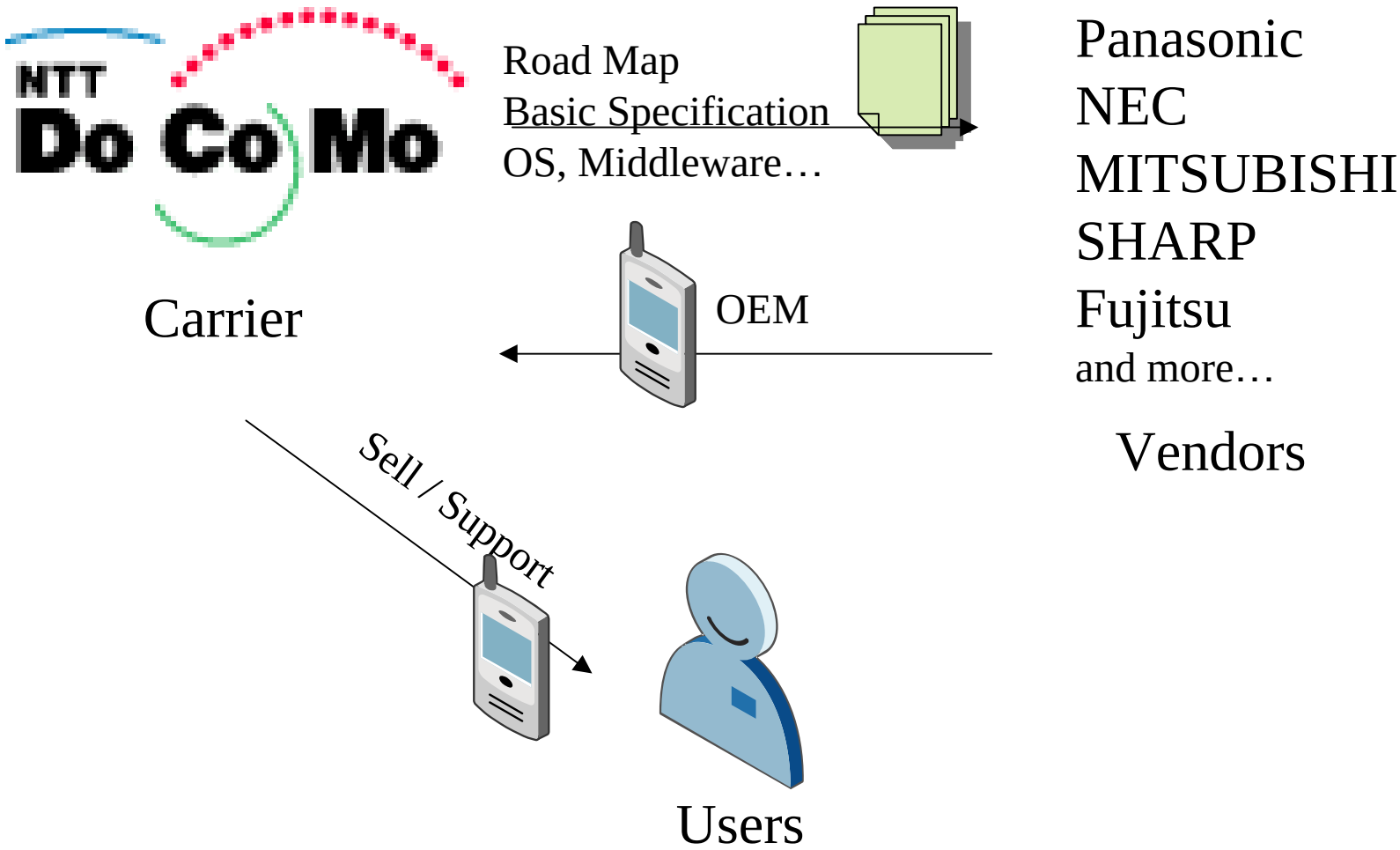
Gathering Information

- NTT DoCoMo does not release details of information about their technologies, including Hardware, Operating System, API….

- But several companies release information. For example….
  - NTT DoCoMo has never publicly announced the use of OMAP processor
  - Texas Instruments press release:

"TI 3G Technology Included in All New Models of NTT DoCoMo's FOMA(R) 901i and 700i Series of 3G Mobile Phones"

Relation


NTT DoCoMo
Carrier
Road Map
Basic Specification
OS, Middleware…
OEM
Sell / Support
Users
Panasonic
NEC
MITSUBISHI
SHARP
Fujitsu
and more…
Vendors

Technologies

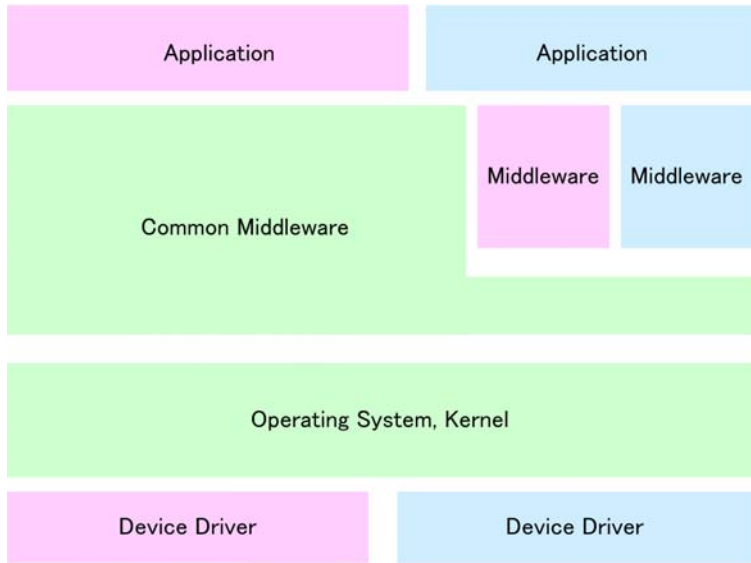
- Hardware
- Operating System
- Software
- Services and Networks

Technologies - Hardware

- 2 CPUs – Communication and Application
  - OMAP (based on ARM) for application
- Felica – contactless IC Card
  - Mainly used for Electronic Cash

Technologies - Operating System

- Symbian
  - Based on Symbian version 6.1
  - UI is original
- Linux
  - Based on Montavista Linux
  - Part of source codes are released with GPL
- BREW
  - Will be released soon



Technologies - Operating System

F901iC based on Symbian

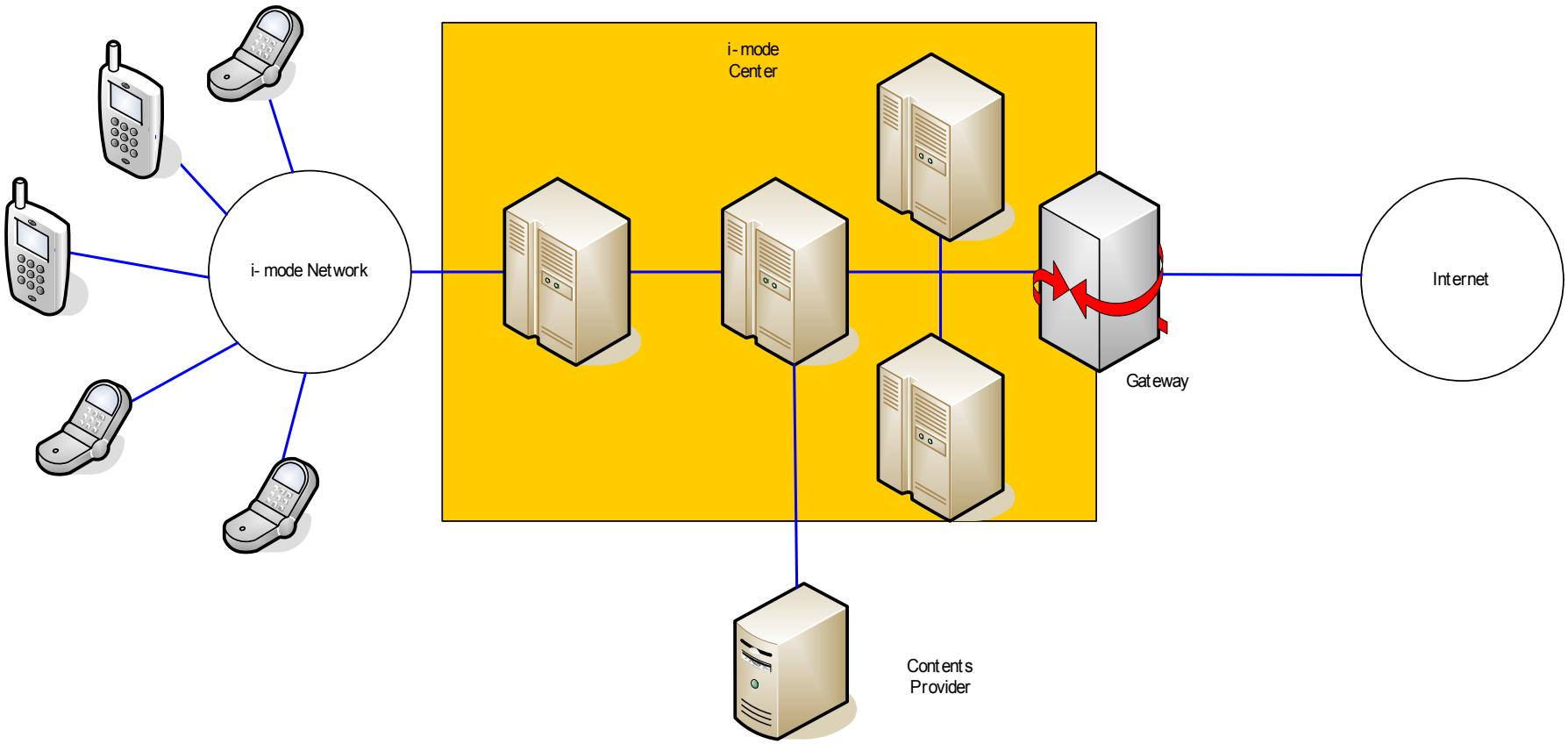
P901i based on Linux

Technologies - Software

- Native application
  - Run on Operating System directly
  - Mail, Browser, Media Player and other
  - No information published
  - Needs to have special contract with NTT DoCoMo
- Java application (i-appli)
  - Run on KVM (K Virtual Machine)
  - DoJa library based on Java 2 Micro Edition
  - All APIs are published
  - Anyone can write and distribute
  - Strong restriction
- Trusted i-appli (i-appli DX)
  - More flexibility
  - Not all Information published
  - Needs to have contract with NTT DoCoMo

Technologies - Services and Networks

- Data communication service “i-mode”



Current Threats

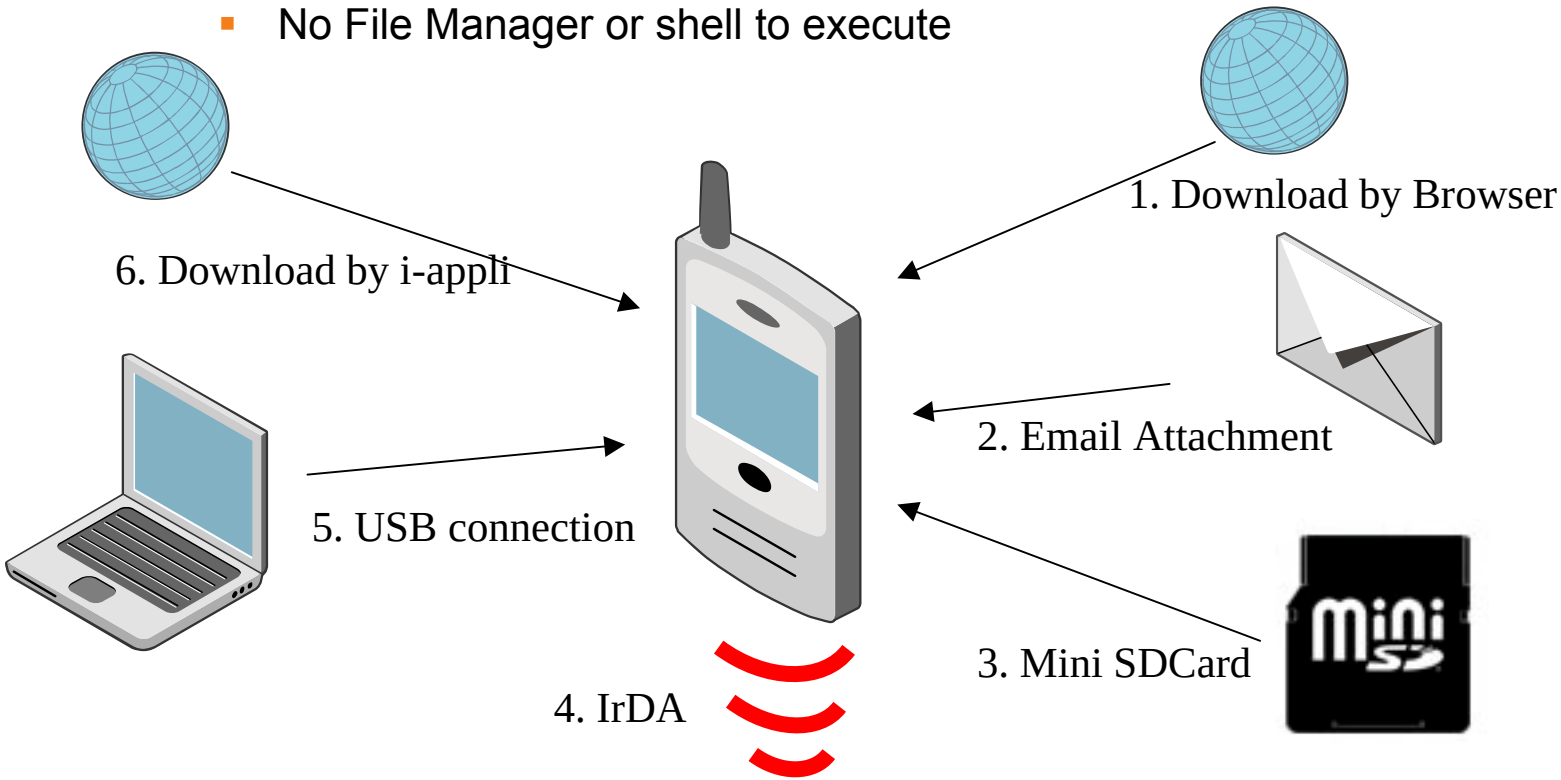
- Does SymbOS/Cabir infect FOMA phones?
- Does Java-based malware run?
- Possibilities of i-appli malware
- Current Security Risk
- SPAM and Phishing

Current Threats – Does SymbOS/Cabir infect FOMA phones?

- No series 60
  - UI is original
- Less Bluetooth support
  - Only one model, F900iT implements Bluetooth
  - Dial-up Networking Profile (DNP), Headset Profile (HS) and Hands-Free Profile (HFR)
  - No File Transfer Profile (FTP) and Object Push Profile (OPP)

Current Threats – Does SymbOS/Cabir infect FOMA phones?

- Unable to install/execute native software
  - Only data files, such as address, sound, movie, and picture files are supported
  - No File Manager or shell to execute



Current Threats – Does Java-based malware run?

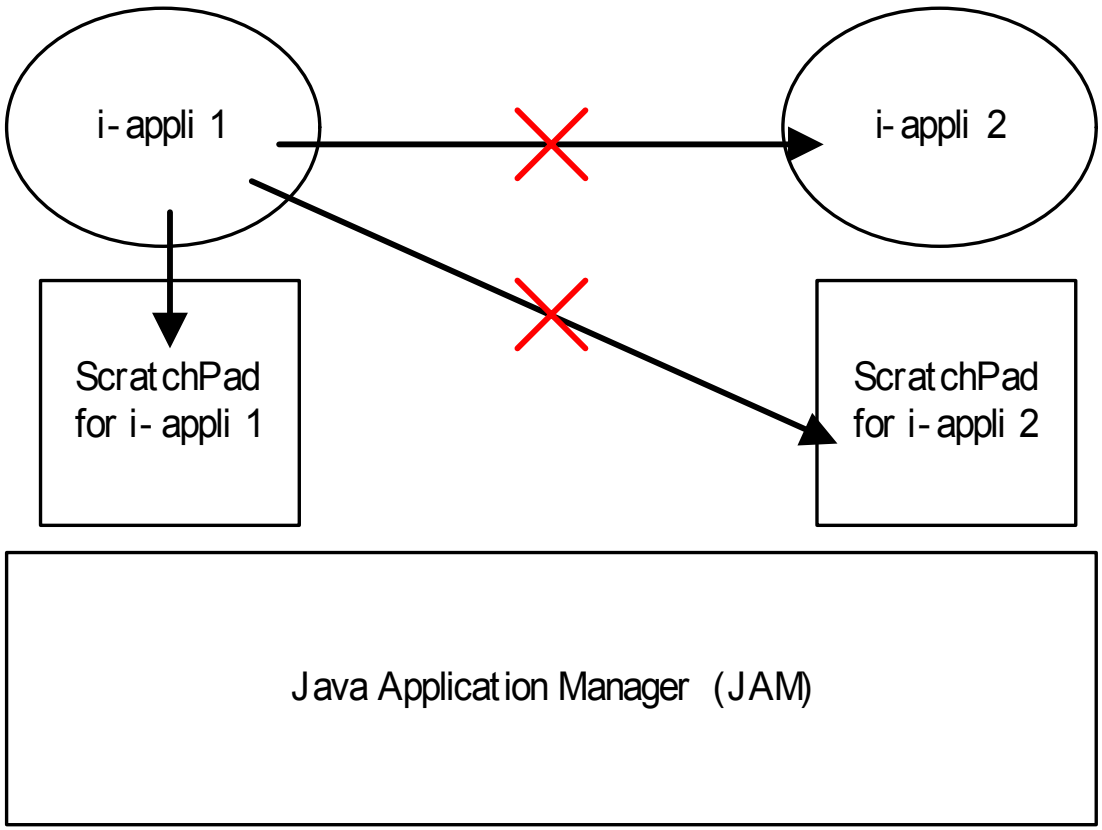
- JAVA/StrangeBrew, JAVA/NoCheat and all other threats do not run
- They target Windows Java platform
- J2ME and DoJa does not fully support all Java APIs
- i-appli needs to inherit IApplication or MApplication CLASS

Current Threats - Possibilities of i-appli malware

- No malware reported since 2001
- Because of strong restrictions

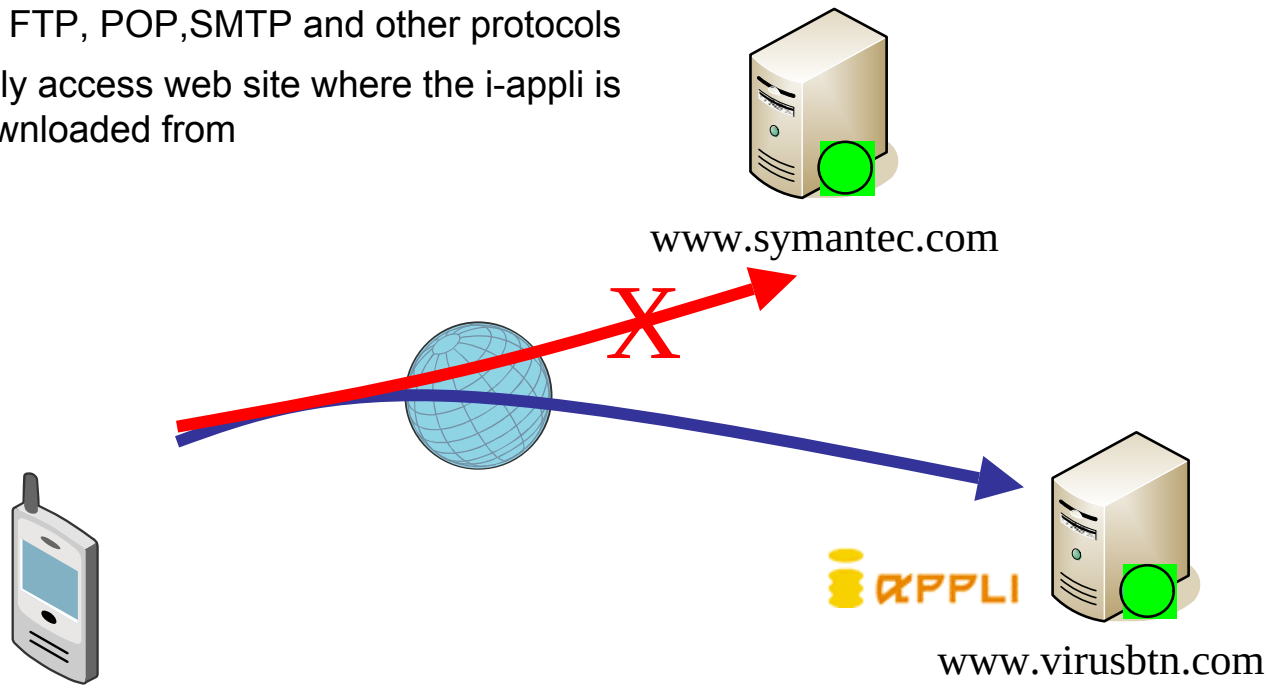
Current Threats - Possibilities of i-appli malware

- File I/O - ScratchPad



Current Threats - Possibilities of i-appli malware

- Network connections
  - Only HTTP and HTTPS
  - No FTP, POP,SMTP and other protocols
  - Only access web site where the i-appli is downloaded from



Current Threats - Possibilities of i-appli malware

- Unable access to native data
  - Address book
  - Bookmark
  - Mail box

Current Threats - Possibilities of Trusted i-appli malware

- Trusted i-appli (i-appli DX)
  - Refer to the address book
  - Send / Receive Email
  - Access any web sites
  - Access data on IC card
  - Needs to be official content provider and obtain 11 digit signature

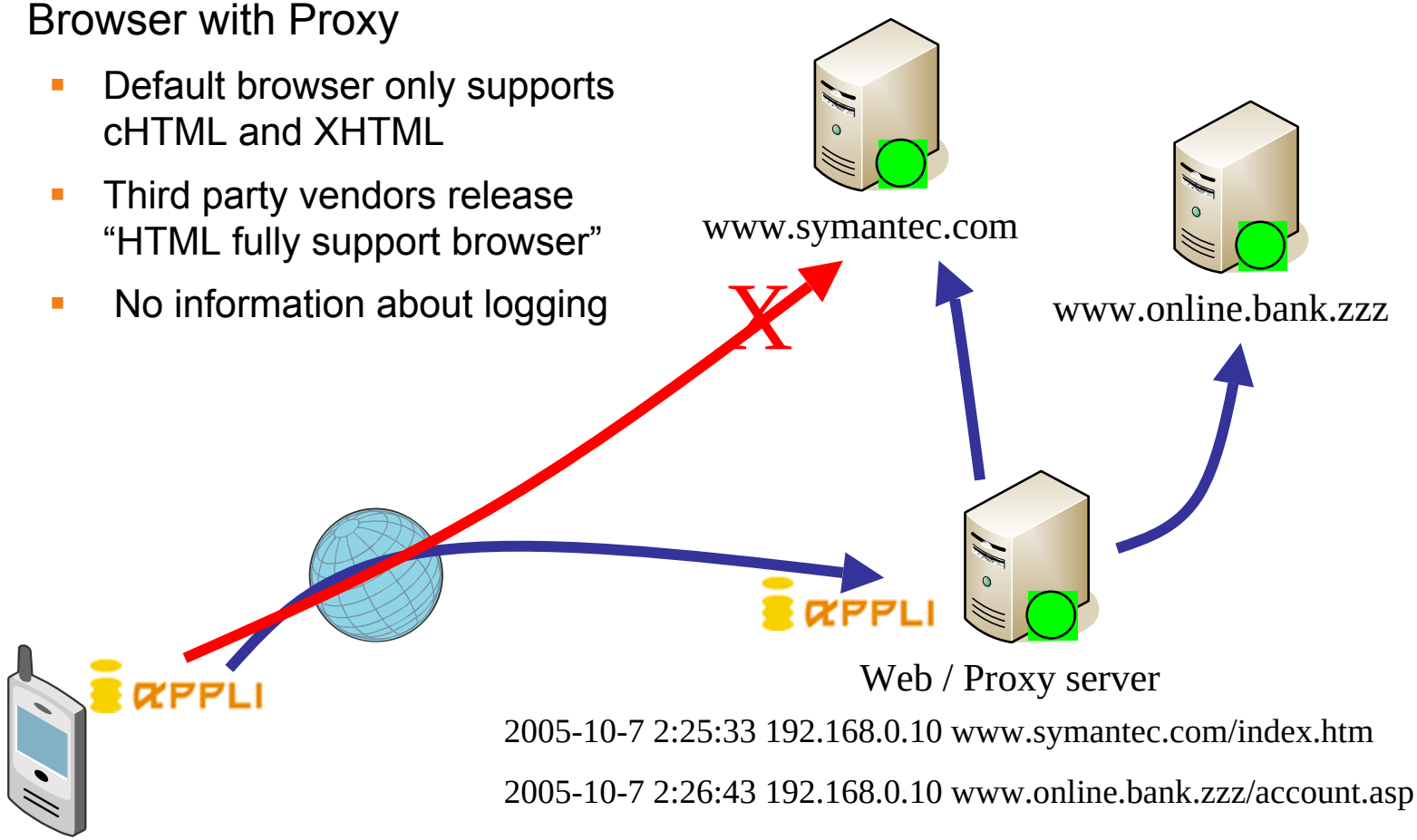
Current Threats - Possibilities of Trusted i-appli malware

- XObject
  - Sensitive data (name, email address, phone number)
  - None of APIs can export the object

- Sending Email
  - MailAgent class is provided
  - Permission required for every mail sent

Current Threats – Current Security Risk

- Browser with Proxy
  - Default browser only supports cHTML and XHTML
  - Third party vendors release “HTML fully support browser”
  - No information about logging

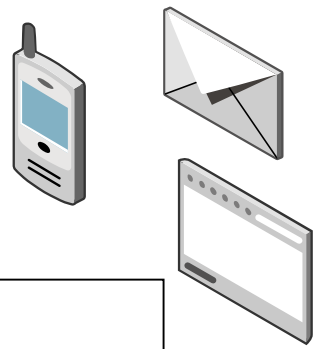


Current Threats – SPAM and Phishing

- Spam
  - 900 millions email every day
  - 95% of email blocked
  - One click frauds
    - Few thousands of victims
    - 660 million Yen damage (4.7 million EURO)

From: xxxx@xxxx.xxx.xxx
To: kaoru_hayashi@yyy.zzz
Subject: See my picture!

Cute Girl … Click here
http://xxx.xxx.xxx/xxx?id=a87sbdsak90sdo1hj



Dear kaoru_hayashi@yyy.zzz,

Thank you for registration.
You are charged with 5000 yen.
Please pay the fee for following account.

kaoru_hayashi@yyy.zzz	a87sbdsak90sdo1hj
lanachan@aaa.bbb	dadoi8adf12msdf3d
piyosuke@ccc.ddd	7faoi9d74098dfandi
turtles@fffff.vvvv	0aoidufaod812s90f9
⋮	⋮

Current Threats – SPAM and Phishing

- Phishing
  - Display screen is small
  - No URL bar in the browser window
  - No one knows where visiting

Future Threats

- Attack against native software
- Risks of electric cash
- Attack against i-mode network
- Wireless LAN spoofing

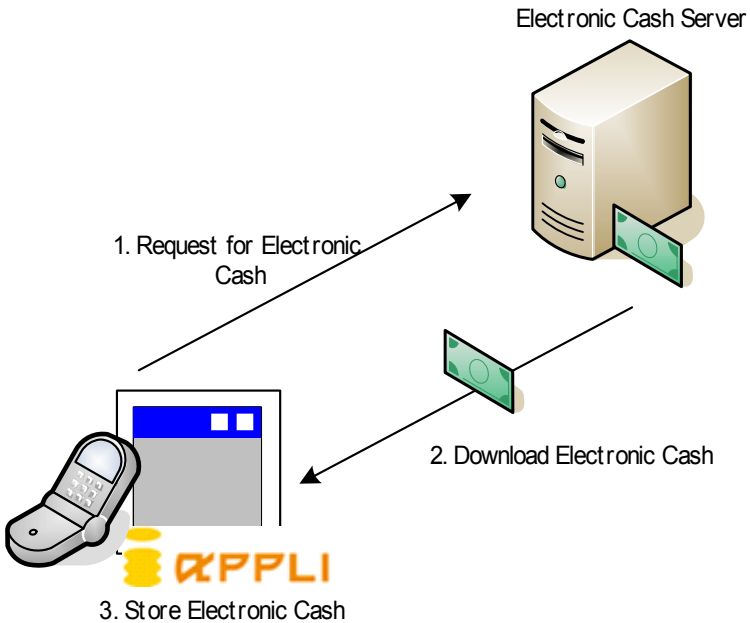
Future Threats

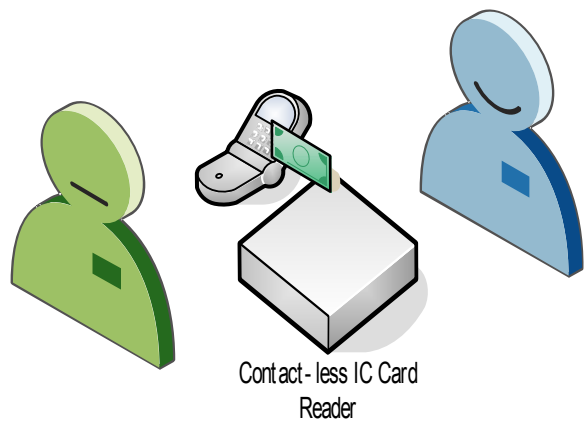
- Attack against native software
  - Size of software increased 15 times in the five years from 1999
  - Error occurring in the software is also increased
  - Denial of service attacks or execution of arbitrary code

- Sony PSP Photo Viewer TIFF File Handling Buffer Overflow
  - Discovered at Sep 26 2005

Future Threats

- Risks of electric cash
  - All high-end models implement contactless IC Card, Felica
  - Trusted i-appli gets cash from server
  - Cash is encrypted on Felica
  - Closing mobile phone on Reader for using cash





Future Threats

- Attack against i-mode network
  - Network is built solidly
  - But information was leaking from one of employee's machine
  - 800 addresses and keys of NTT DoCoMo mobile phone access points
  - By a variant of W32/Antinny

Future Threats

- Wireless LAN sniffing
  - N900iL model implements Wi-Fi
  - For Voice over IP (VoIP) and Internet connection
  - Sniffing conversation and data is likely to increase

Success Factors

- Proprietary system with open technologies
- Publish minimum information
- Fully control all architecture
- Security is priority over flexibility

Security Risks are Business Risk

Appendix

- FOMA M1000
  - First Smartphone from NTT DoCoMo
  - Shipped in August ’05
  - Based on Motorola A1000
  - Symbian OS version 7.0 with UIQ
  - Opera Browser
  - Bluetooth support
  - SDK is provided
  - No connection with i-mode
  - No i-appli environment
  - Under researching

Appendix

- Trusted Mobile Platform
  - Developed by NTT DoCoMo, Intel and IBM
  - Hardware, Software and Protocol
  - No phones based on the specification yet
  - http://www.trusted-mobile.org

- Trusted Computer Group
  - Plan to release “hardware-based security standards for mobile phone”
  - https://www.trustedcomputinggroup.org/groups/mobile

Questions?

- Contacts
  - Email: kaoru_hayashi@symantec.com

symantec™

Thank you!