
FtR of Phenoelit
printer & cellphones
CCC 2003

Java within embedded systems

- The Java platform is the ideal platform for network computing. Running across all platforms -- from servers to cell phones to smart cards -- Java technology unifies business infrastructure to create a seamless, secure, networked platform for your business.

Java Advantages

- Simple
- Distributed
- Portability: Program once, Run anywhere Platform Independence
- Architecture Neutral
- Robust early error checks of the VM takes care
- Multithreaded

HP Printers: ChaiVM [1]

- ChaiVM is a Java Virtual Machine for embedded systems
- HP Printers 9000, 4100 and 4550 are officially supported.
- HP 8150 also runs it.
- ChaiVM on printers comes completely with web server, static files and objects.
- Everything lives on the printer‘s file system.

„In 2001 alone, millions of information appliances will ship with the capability to deliver rich, powerful and dynamic services via the World Wide Web. These appliances are powered by HP Chai embedded software.“

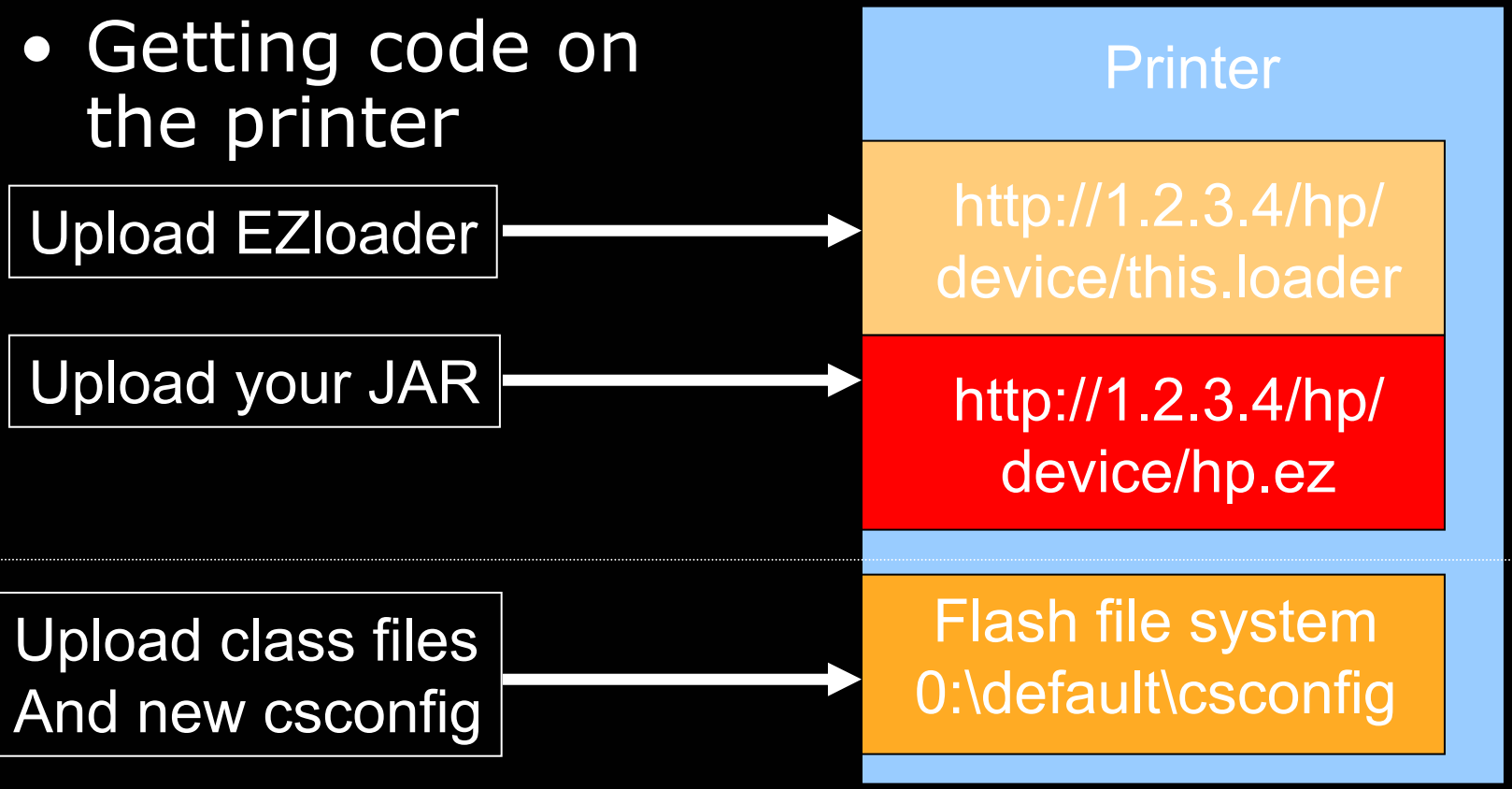
printer & cellphones: CCC 2003 FtR of Phenoelit

HP Printers: ChaiVM [2]

- Chai standard loader service
  - http://device_ip/hp/device/this.loader
  - Loader is supposed to validate JAR signature from HP to ensure security
- HP released new EZloader
  - HP signed JAR
  - No signatures required for upload
- Adding services via printer file system access to 0:\default\csconfig
- HP Java classes, documentation available

HP Printers: ChaiVM [3]

- Getting code on the printer



HP Printers: ChaiVM [4]

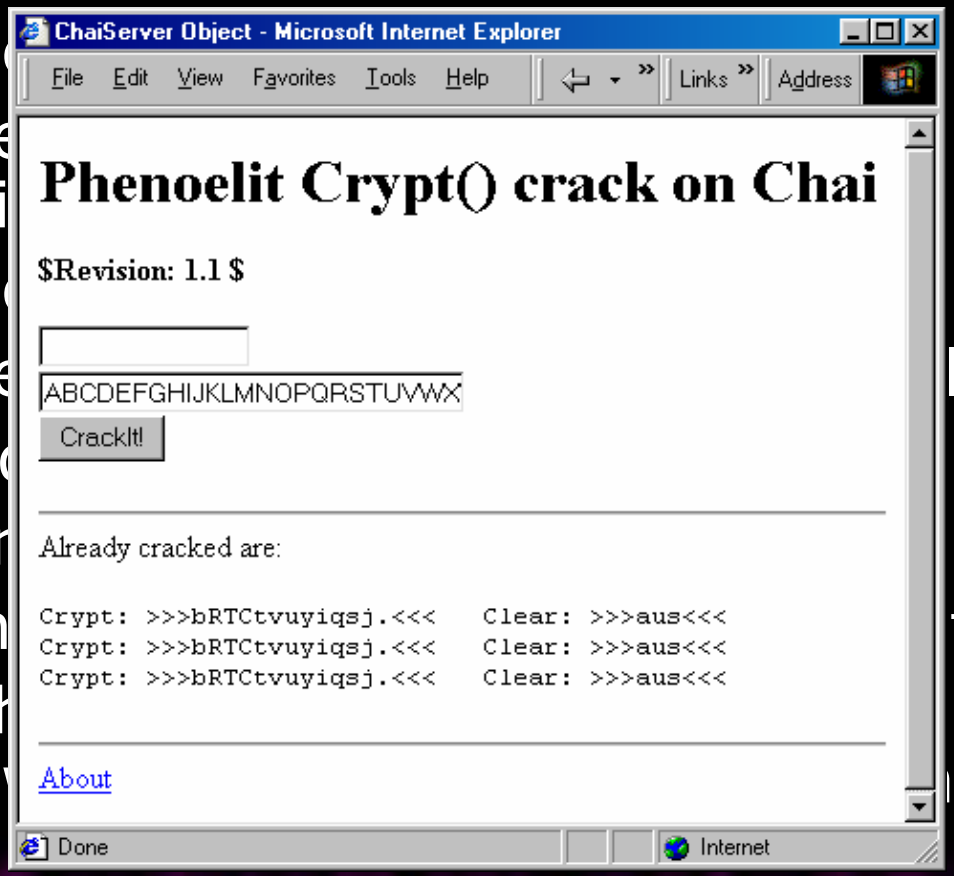
- ChaiVM is quite instable
  - Too many threads kill printer
  - Connect() to unreachable hosts or closed port kills VM
  - Not always throws Exceptions
  - Huge differences between simulation environment and real-world printers
  - Unavailability of all instances of a service kills VM
- To reset printer use SNMP set:
  .iso.3.6.1.2.1.43.5.1.1.3.1 = 4

HP Printers:
Things you can do...

- Phenoelit ChaiPortScan
  - Web based port scanner daemon for HP Printers with fixed firmware
- Phenoelit ChaiCrack
  - Web based crypt() cracking tool
- Backdoor servers
  - Binding and listening is allowed
  - Chai services have access to authentication
- Anything is possible
  (but who wants to code in Java anyway?)

HP Printers:
Things you can do...

- Phen
  - We n for HP Pri
- Phen
  - We l
- Back
  - Bir
  - Ch thentication
- Anyth
  (but yway?)



printer & cellphones: CCC 2003 FtR of Phenoelit

Siemens S55 – feature list [2]

- the normal stuff
  - Phone book
  - SMS
- The new stuff
  - MMS
  - WAP
  - GPRS
  - Email client
  - Bluetooth
  - Java™ Wireless Technology

Siemens S55 – feature list [2]

- t
- Th

„ The sleek S55 uses the latest Java™ technology, to choose among plenty of practical business, travel and entertainment applications as well as games…“s

S55 Java API

- Provides access to nearly all functionalities of the phone
  - com.siemens.mp.gsm.PhoneBook
  - System.getProperty()
    - International Mobile Equipment Identity
    - ...
- Most classes created under „com.siemens“
- Siemens provide devl. environment: The Siemens Mobility Toolkit (SMTK)

S55 How to get a your application to the phone?

- Sell it as a game ...
- WAP
  - Link to a "Java Application Descriptor" .JAD
  - Phone will grep the Java Archive JAR
- Data wire

Does not work

S55 JAD parser

- Flaw1
  - No MIDlet-Name
  - No MIDlet-1
  - Give a blank and
  - idling display
- Flaw2
  - MIDlet-Name of more than 120 chars
  - Create a directory overflows the name of
  - the file. -> format file system to delete

```
MIDlet-Version: 1.0.0
MIDlet-Vendor: Phenoelit
MIDlet-Jar-URL: Test.jar
MIDlet-Name: evil
MIDlet-1: evil,,evil
MIDlet-Jar-Size: 2791
```

S55 Send a SMS

- JAVA class for sending SMS: com.siemens.mp.gsm
- JAVA is threaded -> Race conditions
- The „Message Box“ is faster
- The normal Canvas comes later

Java summary

- The Java API's on embedded systems will provide you a good interface to increase the functionality.
- No exploiting, no Shellcode, no OPCode
- Find a way to deliver you application

S55 Bluetooth

- New „Paired Devices” will create a Message box
- Randomly created „Paired Devices“ will display up to 20 Boxes on top of each other
- Looks like a crash
- Takes all kind of data provided with the Object Exchange Protocol (OBEX)
- Tested with 1200 business cards
  - Max number for deletion 256
  - Removal via IRDA easy ...

S55 Business cards

- Empty card will disable the will disable the functionality completely if saved
- No Way to remove that card except power cycle

```
BEGIN:VCARD
VERSION:2.1
N:
FN:
ORG:
TITLE:
TEL;WORK;VOICE:
TEL;HOME;VOICE:
TEL;CELL;VOICE:
TEL;WORK;FAX:
ADR;WORK:;;;;;;;
LABEL;WORK;ENCODING
=QUOTED-PRINTABLE:,
EMAIL;PREF;INTERNET:
END:VCARD
```

S55 GIF Renderer

- GIF contains values for the positioning
- 0xFFFF as Value will crash the whole phone
- can be submitted as MMS
- Further research for exploitability needed

Cell phones summary

- I want a phone to do a call an store some addresses that‘s it
- The new UMTS phones will be fun as well
- Never ever trust a JAVA Game ...


Phenoelit
Special thanks to:
Internet
Menu