Security Analysis Of Handhelds

Vaibhav Bhandari
Department of Computer Science, UCSC
vaibhav@soe.ucsc.edu

November 29, 2001

Embeded Devices are everywhere

We can't built secure applications on these in-
secure devices.

Introduction

- Threat : Causual / Determined

- Security : Restricted / Confidential

Exemplary Handhelds

- Palm OS device: Monolithic OS
- Simputer: Mass market PC with full-fledged OS support

Security Analysis

Evaluating the robustness of security policy to handle the various threats.

Making certain the robustness of various security mechanisms and understanding there limitations.

Questions to answer

- Does it have a power-on password and is the password verification robust?
- Is there access control for local/ remote operation?
- Is there a way to check Malignant programs?
- Is Strong Encryption available for both wired and wireless links?
- Is Memory properly secured?
- Is there a cyrpto-processor and how vulnerable is it?
- Are the device protocols time/tool tested?
- Is there any audit mechanism available?
- Does the device have access to updated information?
- Finally, how robust are the business process?

Secure Password Retrieval

- Challenge/ Response mechanism on the network.
- Encrypt and Salt Credentials stored on the system.
- Implementation of **power-on** passsword.
- Alternative passwords like signatures, graphical passowords.

Access Control

- Palm: password protected data -records and beam bit.
- Simputer: Session database.
  - Name
  - Magic: read(r), exclusive(e), secure(s), transient(t)
  - Value
  - An example of a table is given below:

Name	Magic	Value
name	s	Manohar
address	s	CSA Department
DOB	s	June 21 1960
Status	e567rty	Married
phone	ru87iii89	3092368
choice	t345tyu	pizza

- IML code segment using it:

```
<page>
 <tr><td> Name: </td><td><input type="text" width="15"
 height="1"
var="var0" value="_name" magic="s"/></td></tr>
 <tr><td> Occupation: </td><td><input type="text"
 width="15" height= 1"
var="var0" value="_occupation" magic="s"/></td></tr>
</page>
```

- Transfer of data to an application (especially remote) is through express approval of user.

Smart Card Attacks

- Invasive attack on Hardware:Using devices like scanning capacitance microscope can fuel low-cost attacks.

- Non-invasive hardware attack: like analysis of power consumption will fade due to counter attacks like randomised clocking.

- API-level attacks: Chained processing commands in unusual way based on:
  - Data Repeats: exploiting X-OR vulnerability
  - Timing
  - Man in middle

An Authentication Protocol

$$
\begin{array}{lcl}
\mathsf{U} & \Rightarrow & SC : PIN \\
\mathsf{SC} & \Rightarrow & D : UserValid \\
\mathsf{D} & \Rightarrow & SC : K_{PD}, D_{SN} \\
\mathsf{SC} & \Rightarrow & D : \{N, SC, K_{PD}, D_{SN}\}_{K_{SU}}, K_{PU} \\
\mathsf{D} & \Rightarrow & CA : \{N, SC, K_{PD}, D_{SN}\}_{K_{SU}}, K_{PU} \\
\mathsf{CA} & \Rightarrow & D : \{GoodD\}_{K_{PU}} \\
\mathsf{D} & \Rightarrow & SC : \{GoodD\}_{K_{PU}}
\end{array}
$$

In **BAN** Logic:

$$\frac{\text{(SC believes good User) (SC believes CA said good Device)}}{\text{SC believes good Device}}$$

Acknowledgements

Thanks every one, especially Prof. Martin Abadi and KS Vivek of PicoPeta Simputers for support and ideas.