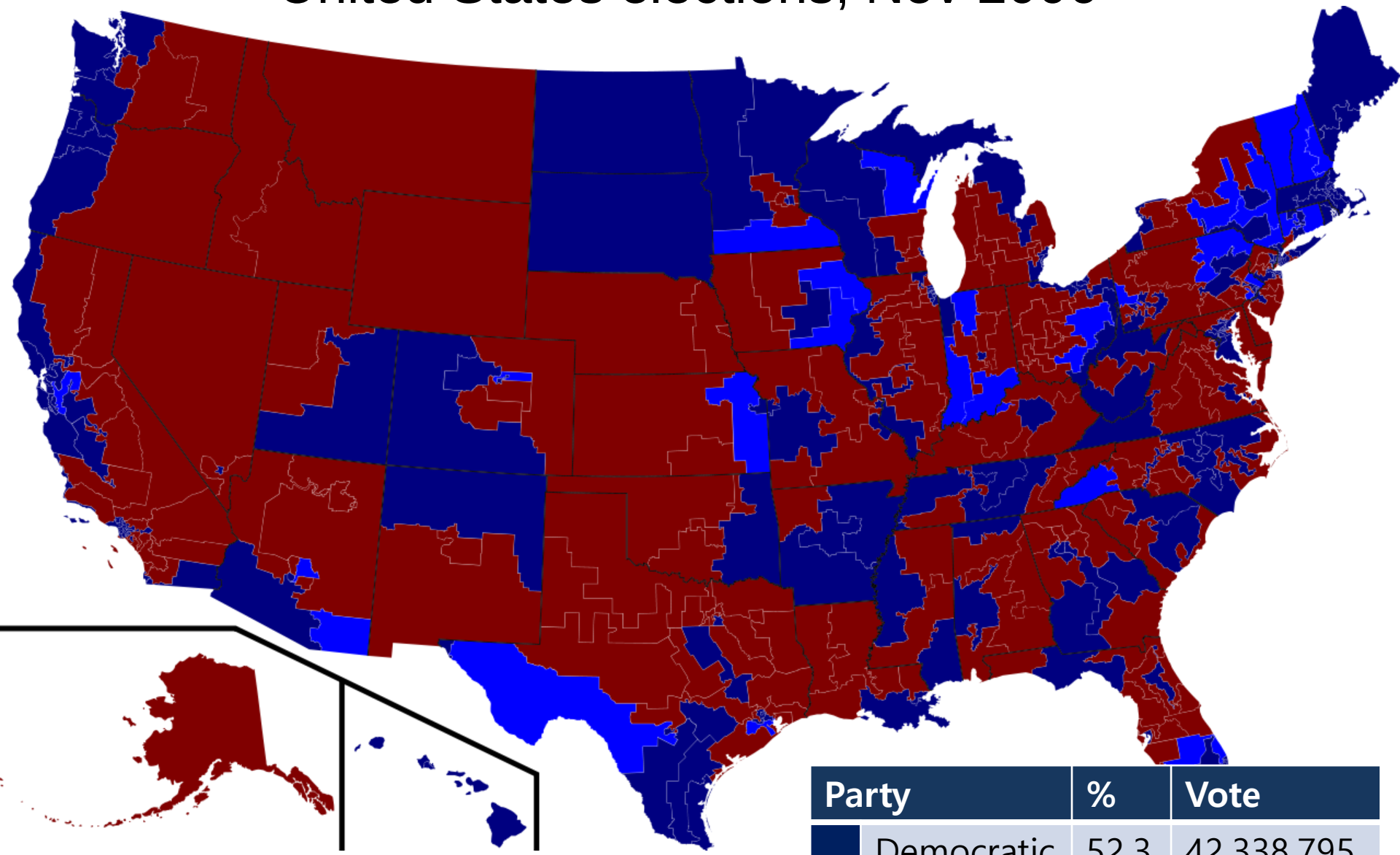
Security Analysis of the Diebold AccuVote-TS Voting Machine

EVT '07
A. Feldman, J. Halderman, and E. Felten

Presenter
Jinseob Jeong

This file is originally written by Dawon Park and Donhwan Kwon,
Revised by Jinseob Jeong

United States elections, Nov 2006



Party	%	Vote
Democratic	52.3	42,338,795
Republican	44.3	35,857,334

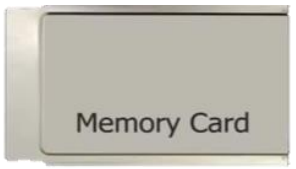
Voting

Paper-based Voting

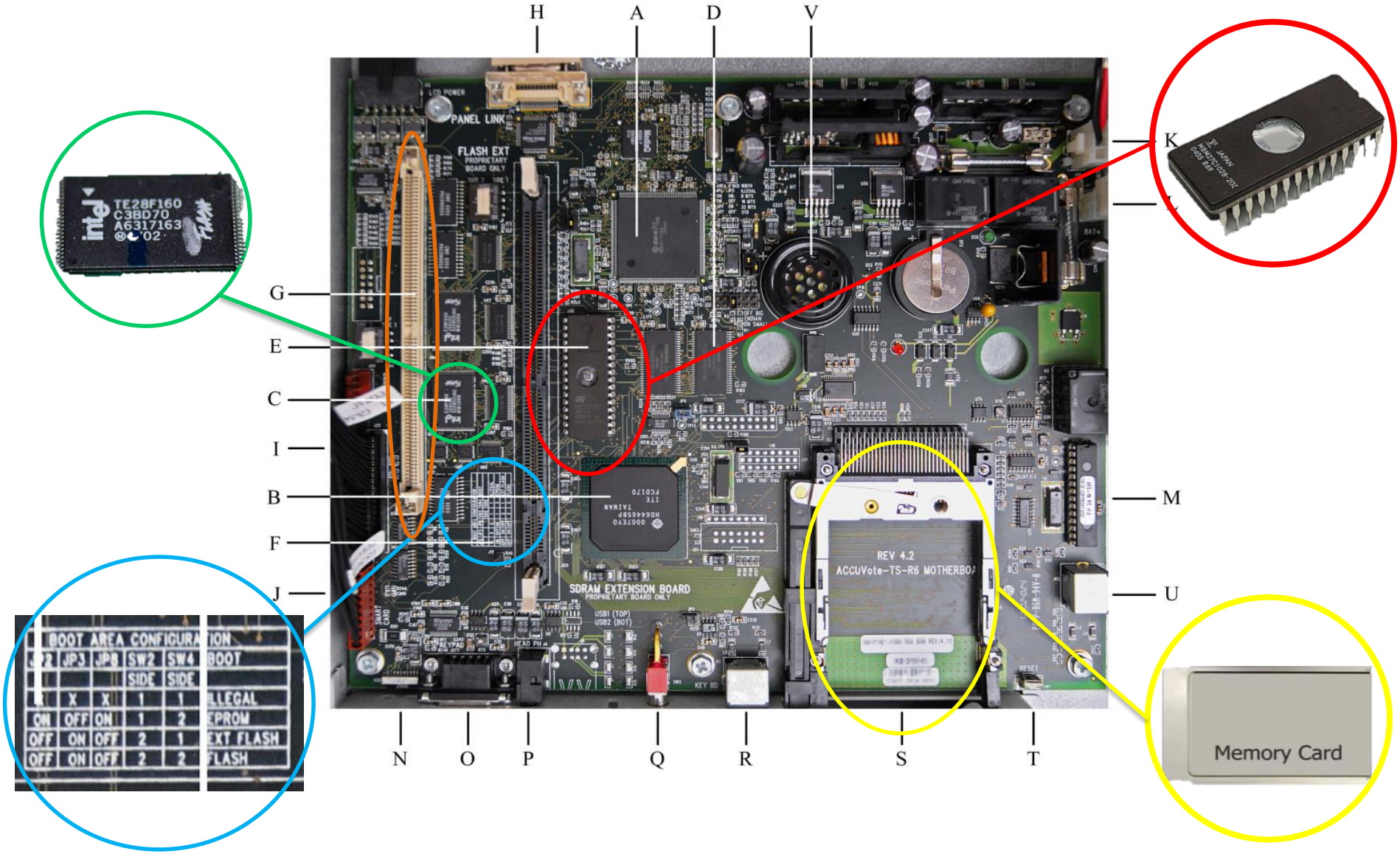
Electronic Voting

AccuVote-TS Voting Machine

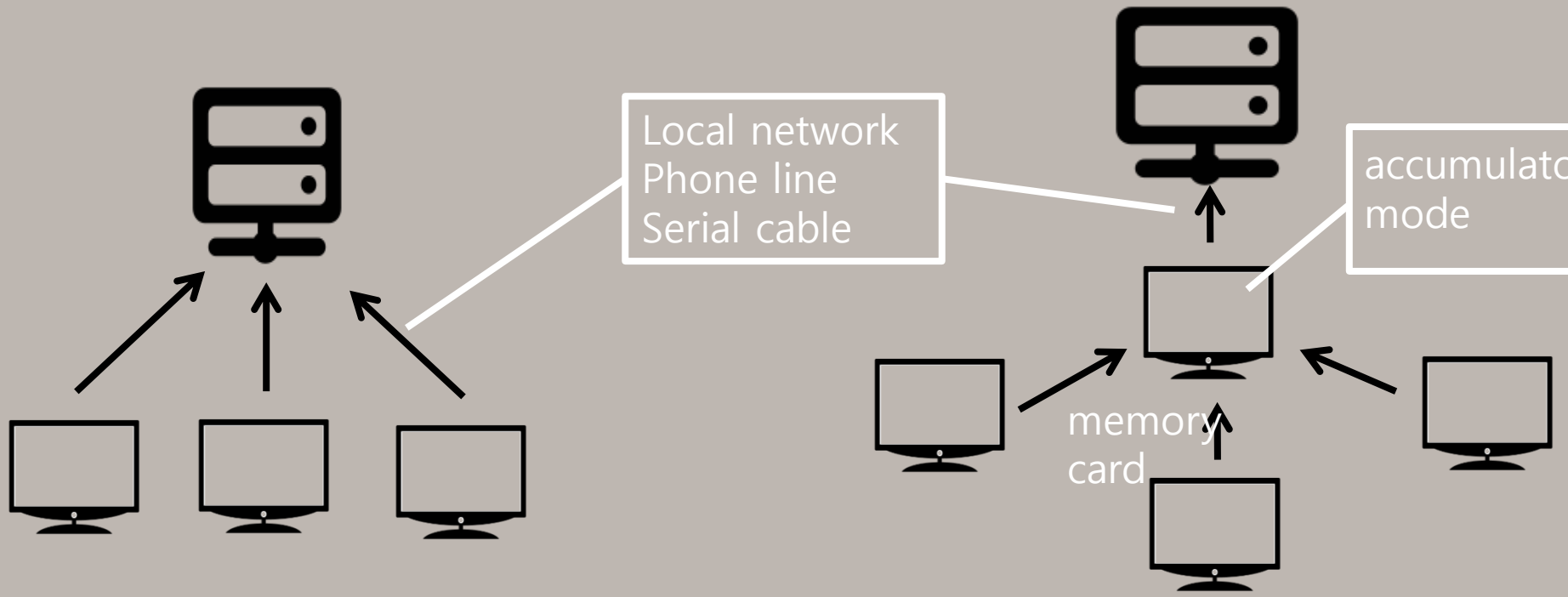
Software	Software
Windows CE	
Direct Recording Electronic (DRE)	



AccuVote-TS Voting Machine



AccuVote-TS Voting Machine



- Voter access card (valid -> invalid)

- **On-board Flash memory, Flash memory card**

- Local network
- **Accumulator mode**

Attacker's Goal

Attacker's Goal

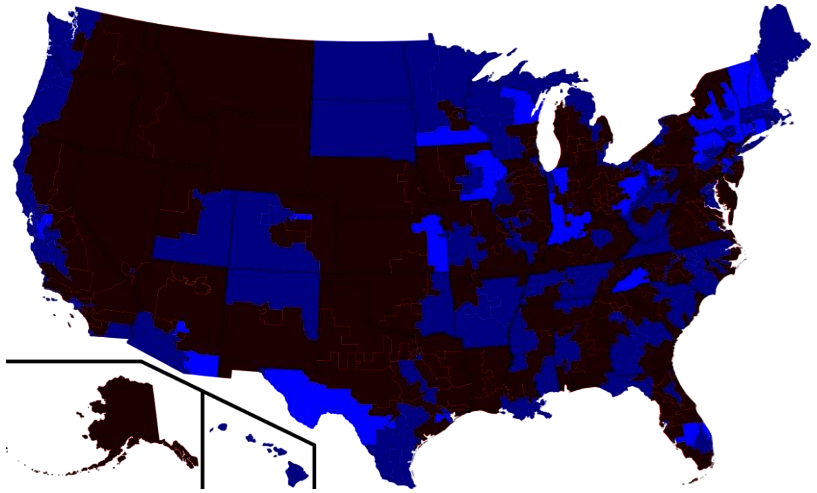
Vote Stealing

Party	%	Vote
Democratic	52.3	42,338,795
Republican	44.3	35,857,334

5% (4,048,777)

Party	%	Vote
Republican	49.3	39,906,111
Democratic	47.3	38,290,018

Denial of Service



Vulnerability

Direct Installation

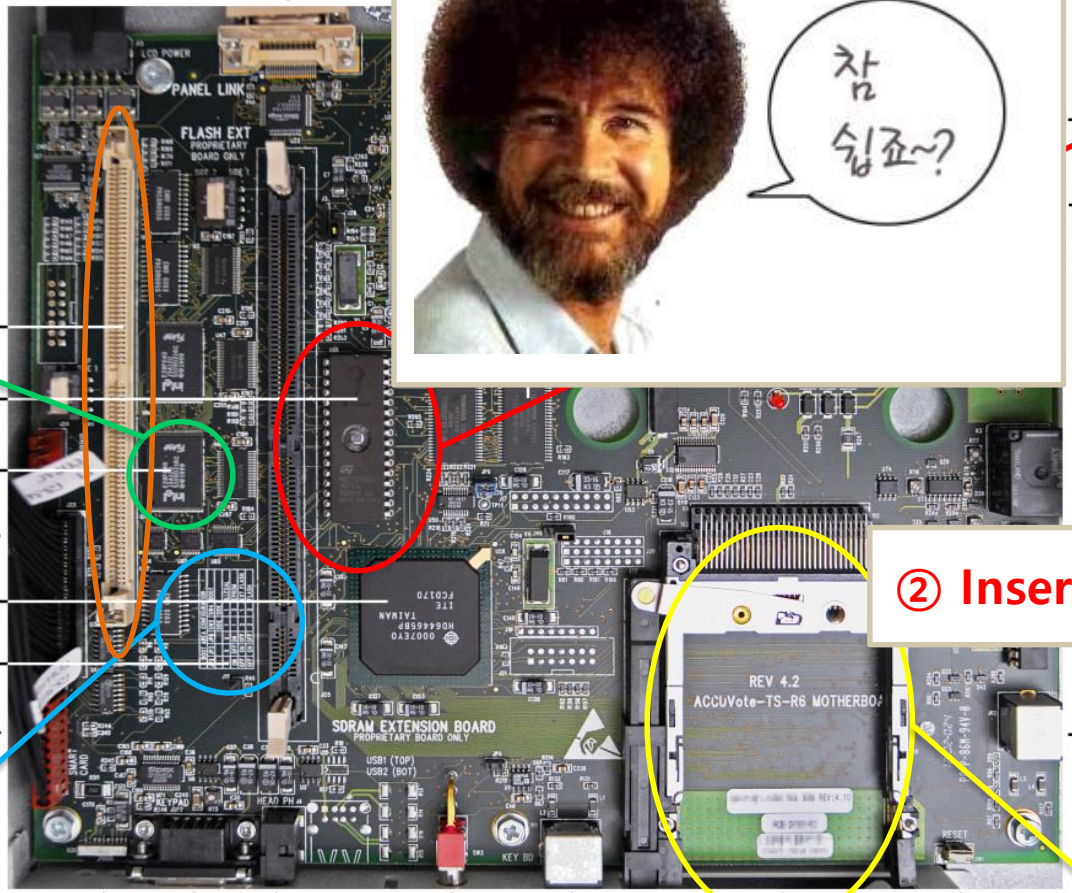
- Easy to physically access to the motherboard
  - EPROM chip, removable memory card, power button
- Source of bootloader code is changeable
  - EPROM chip / On-board flash memory / Memory card
- Not verify authenticity of files
  - fboot.nb0, nk.bin, EraseFFX.bsq, explorer.glb, .ins file

Spreading Virus

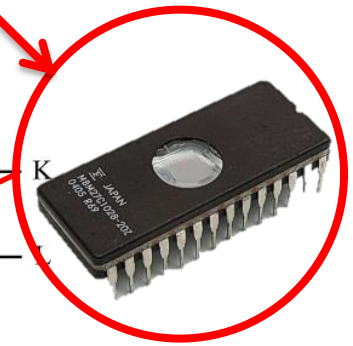
- Removable memory card can spread out virus
  - Used for multiple machine, rewritable memory

Attack Scenario – installing malware

Attack Scenario – installing malware



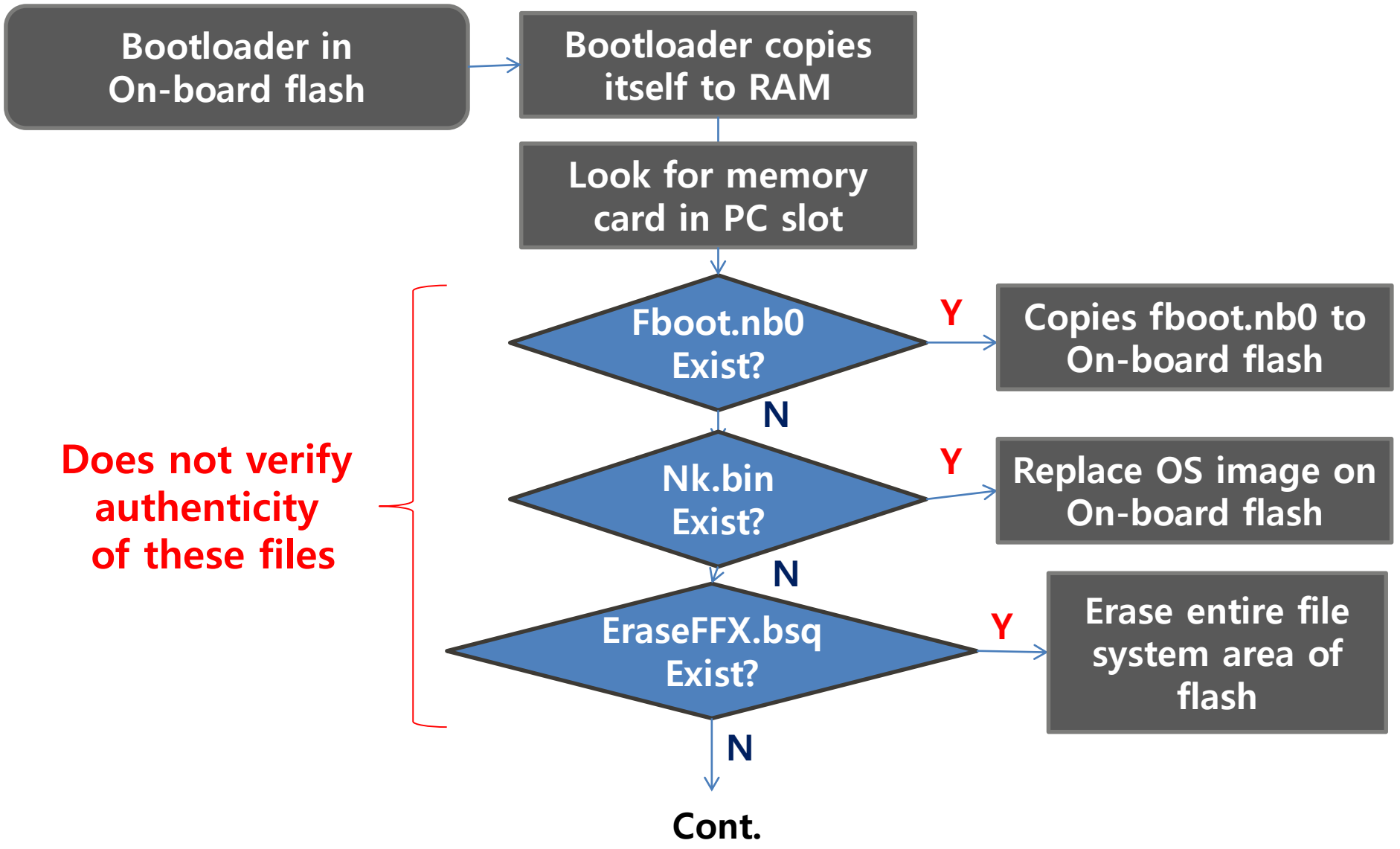
① Replace EPROM chip



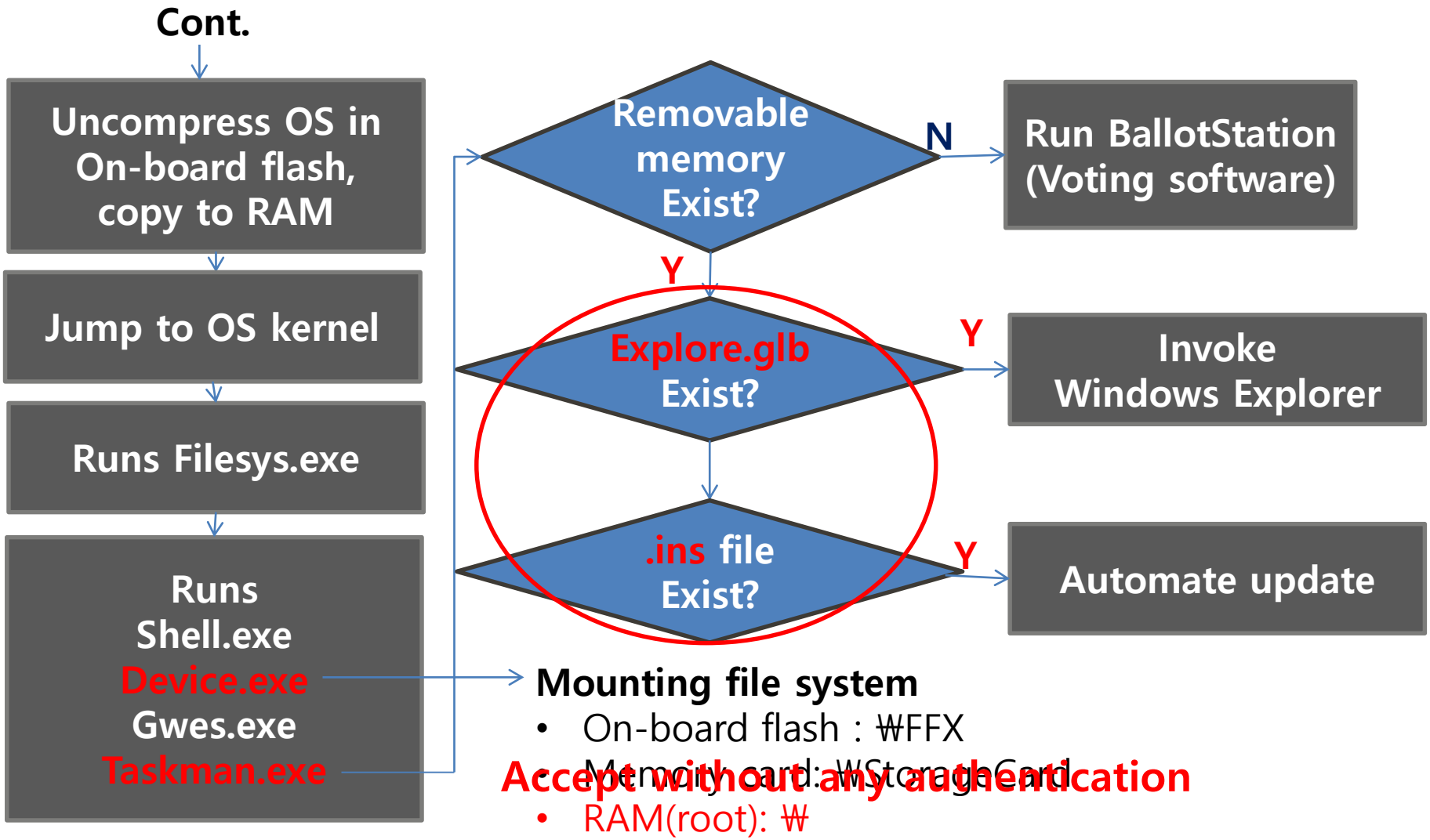
② Insert Memory Card

Determine source of bootloader code

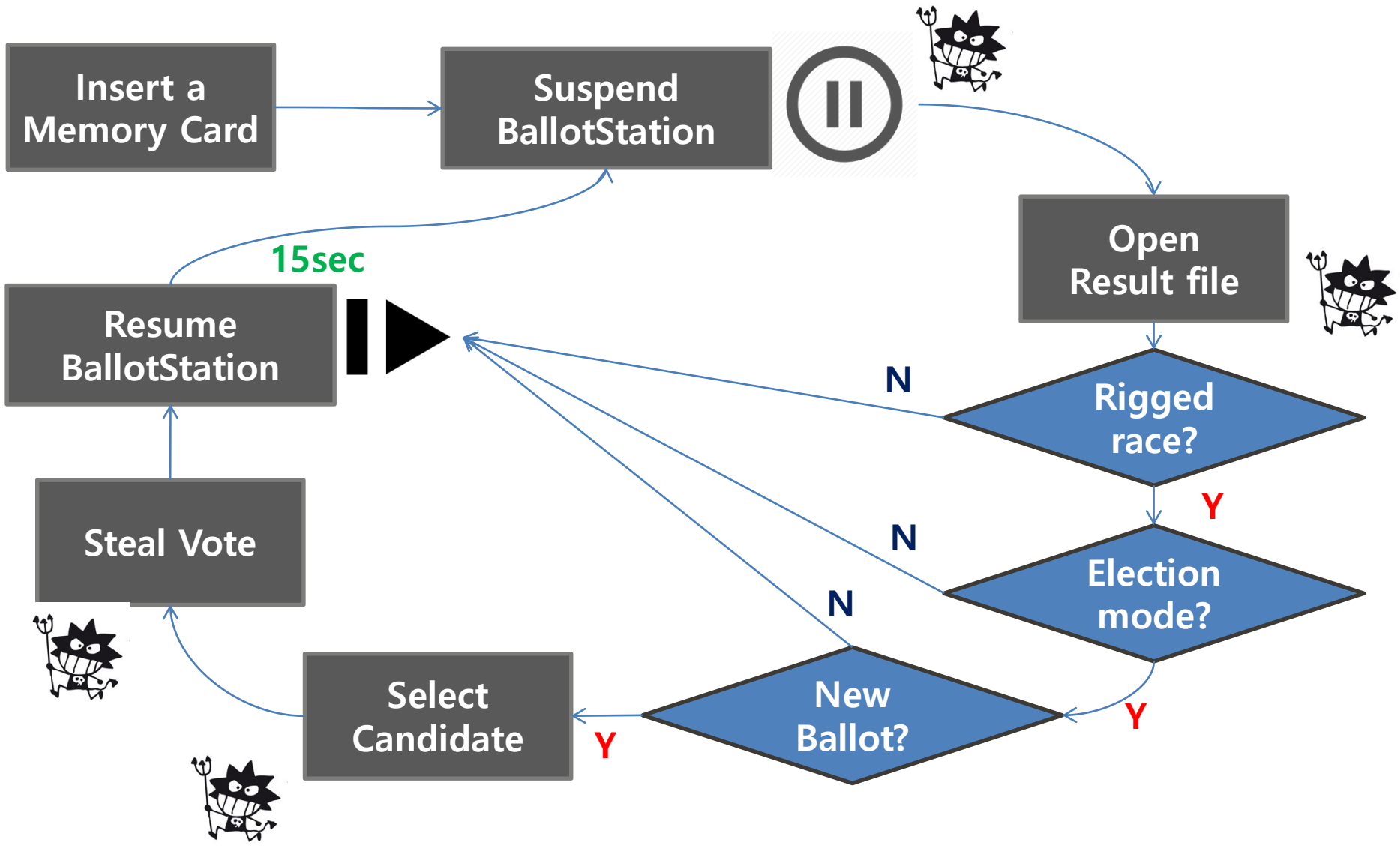
Attack Scenario – installing malware



Attack Scenario – installing malware



Attack Scenario – stealing vote



Mitigation

- S/W & H/W modification
  - Code signing & signature verification
  - Person confirm for software updates
  - Not use rewritable storage -> tamper-proof logs, records
- Physical access control : broken seal cause DoS
- Parallel testing : simulation pattern, secret knock
- Effective certification system : Strong Certifica
- Software independent design : printout paper

Conclusion

- H/W & S/W encompassing study of a widely used DRE
- Demonstration of vote-stealing and virus spreading
- Warning for large scale fraud
- Proving H/W architecture limitation of the target

Limitation & Future work

- General attack idea -> Attack through network
- Malicious action of voters : copy card or re-enable invalid card
- Physical access is not so easy during voting

Another Story – Diebold

`02 `03 `03

Diebold Election Systems to Become Premier Election Solutions

Increased Operational Independence, Concentrated Focus on Elections Systems

Industry Will Strengthen Premier's Competitive Advantage

Aug 16, 2007, 01:00 ET from Premier Election Solutions, Inc.

None of them

Diebold CEO resigns after reports of fraud litigation, internal woes

John Byrne

Harri Hursti
- **Hardware & compiled boot-loader**
- Problems with software update

Feldman, Halderman, Felten
- Reverse engineer hardware & software
- Confirmed earlier studies by **demo**

Another Story – Diebold

`07

David Wagner, California
- **TTBR(Top to Bottom Review)**
- "Deep architectural flaws"
- Buffer overflow, weak cryptography

`07

Ohio
- Project EVEREST
- "Yet more vulnerabilities"

`09

Election Systems & Software
Take over

`10

Dominion Voting System
Take over

Electronic voting in Korea

Secure?

OOO 당, 왜그러나 또 '선거 조작?'… '1번이 ooo 선장' 괴문자 파문

K-보팅 주소도 그대로 노출됐다. 비밀 보장을 위해 각 유권자에게 알파벳 6자리로 된 고유번호와 보안코드가 제공됐음에도 특정인의 비밀코드가 고스란히 노출돼 클릭하면 자동 연결된다.

'나가수' 뽑은 선관위 전자투표 보안기술 엉터리

Thanks