APT defense from the view of security architecture

Kiyoung Kim

2013-7-20

Cyber starts from Real World

Some says cyber is more real than real world
Some says they will merge & integrate
But
During transition some important things are
Missed or misinterpreted

Differences in Eastern and Western Philosophy

善不善

Originally (East) → **Good and Not Good**

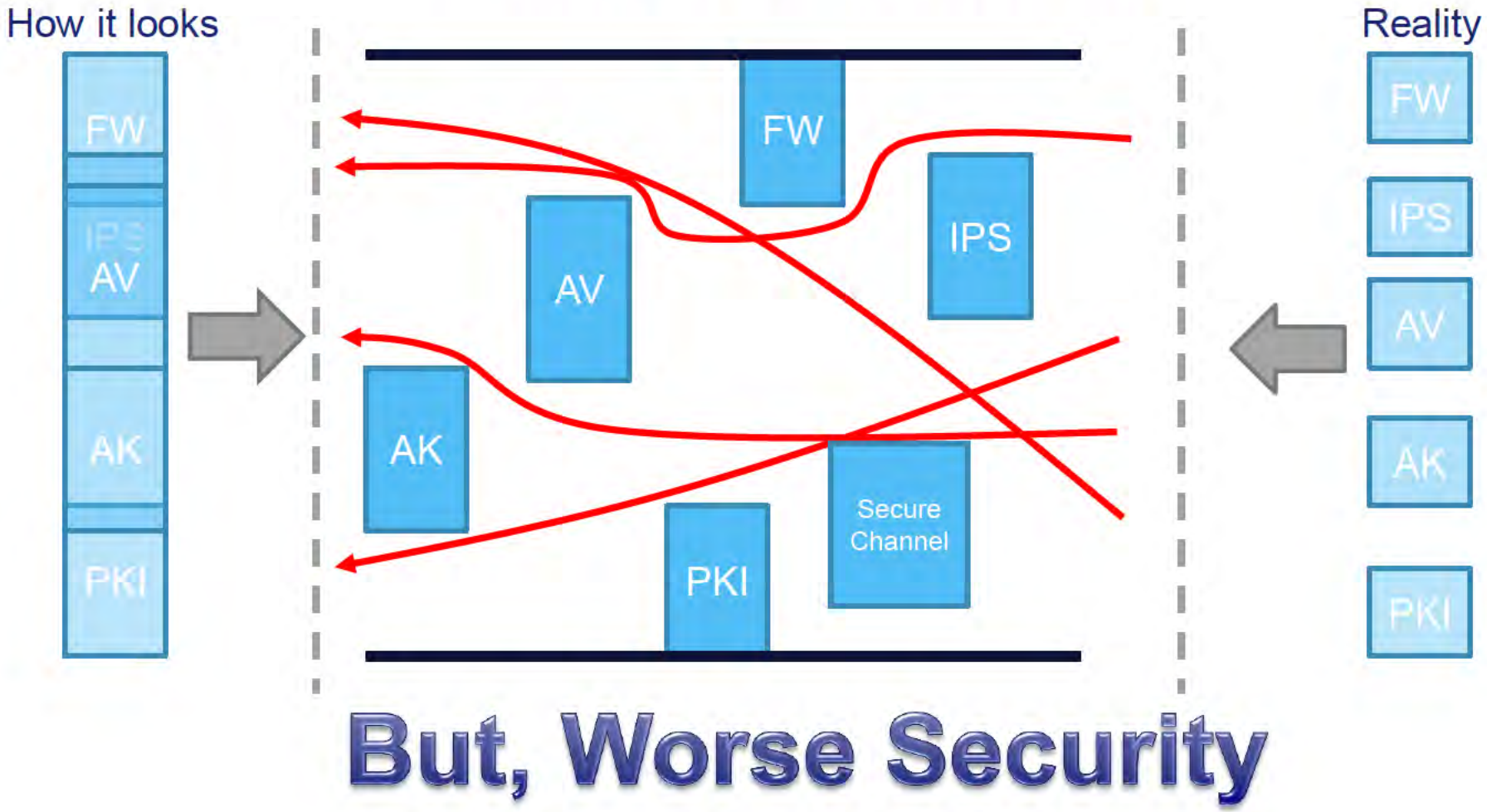
↓

English (West) → **Good and Evil**

Dichotomous Thinking

Result of Dichotomous Thinking

Better Solution



But, Worse Security


Like this!


STOP
AND
THINK

Controlled Variable

Theories tend to be qualitative in nature under controlled variables

But real world is complex system.
And when theories are applied at the same time
The result shows non-linear pattern.
Almost unexpected

The Chaos

When the present determines the future,
but the approximate present
does not approximately determine the future.

From : http://en.wikipedia.org/wiki/Chaos_theory

it must have the following properties:
it must be sensitive to initial conditions;
it must be topologically mixing; and
its periodic orbits must be dense.

State of Current Defense System

We have to know facts more correctly

Which means, we have to handle many things at the same time


FACT

Even with so many layered solutions

Attackers never fail to arrive to victim's PC

Bit9 (Feb. 2013)

- Breach used to collect company certificates
- Certificate used to bypass Bit9 protection at customer sites

New York Times (Feb. 2013)

- Initial infection via SpearPhishing attack
- Coincided with news story on Chinese Prime Minster

StuxNet (Jul. 2010)

- Iran's SCADA controlled nuclear facilities targeted
- Iranian nuclear program halted

EMC/RSA Breach (Mar. 2011)

- Security company RSA (a Unit of EMC) breached
- 2-factor authentication information stolen

And also in Korea

Use any resource if possible …

NongHyup(320) (Mar. 2013)

- Through web and then file dispatch system
- Web and ATM service halted

Korea Gov. Bidding (Apr. 2013)

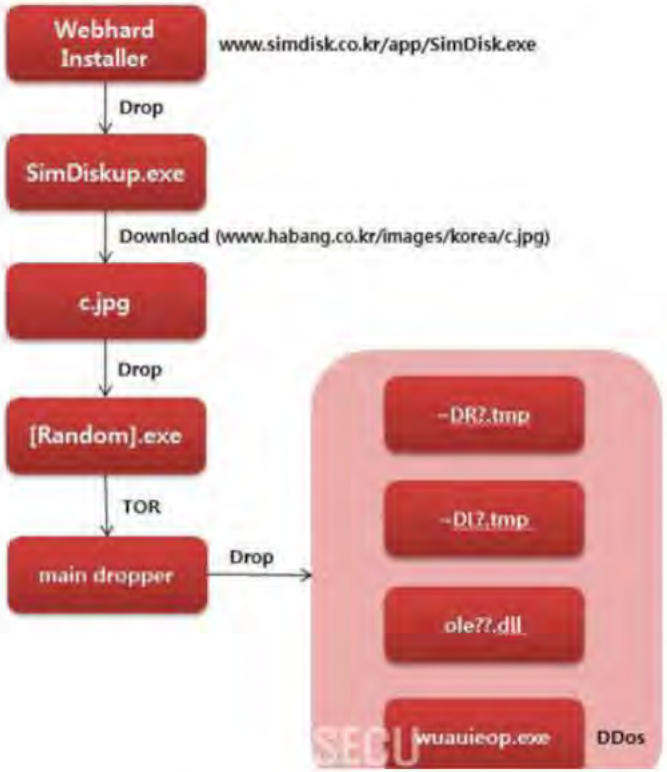
- HWP exploits and usb for several years
- Revealing Construction Bidding Information

625 Cyber terror (Jun. 2013)

- Drive by, exploit of sw update system
- Deface, system halted

Some companies say they can block the attack, but …

625 cyber terror



By-passed anti-apt solutions

We need to take a time break

And make Tactic

We already know, our solutions can be easily penetrated

Why don't you accept it?

It doesn't mean surrender!

Even in Computer Games Formation is important!

What are they saying?

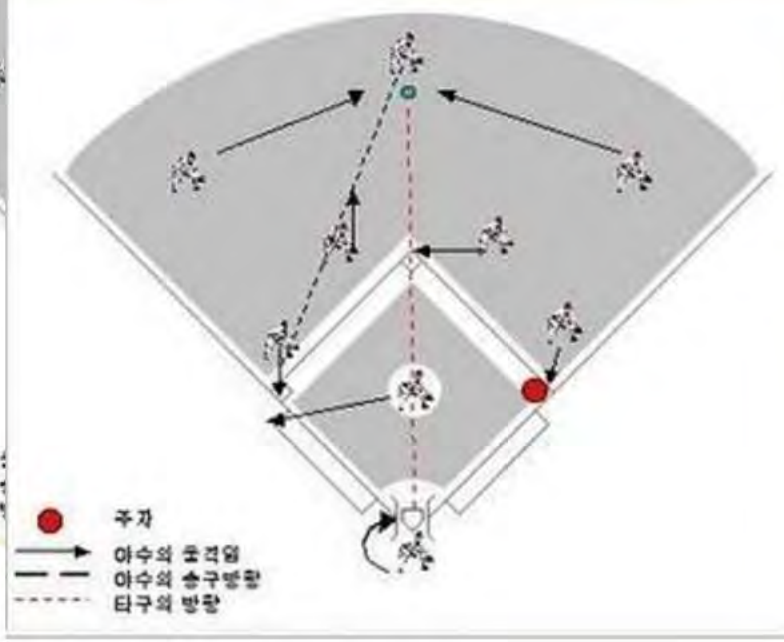
Then how should we move?

주자2루 또는 주자 2,3루에 있을 때 3루간을 빠져나가 좌익수 쪽에 단타가 낮을 경우.

주자가 없는 상황에서 좌익수 쪽에 단타가 낮을 경우

주자 없을 때 중견수 앞에 단타가 낮을 때.

주자가 1루에 있을 때 중견수 앞에 단타가 낮을 경우.



투수: 3루를 커버한다.
포수: 홈을 방어한다.
1루수: 1루를 지킨다.
2루수: 2루를 지킨다.
3루수: 3루를 지킨다.
유격수: 중견수로부터 송구된 공을 중계한다.
외야수: 좌익수와 우익수는 중견수를 커버한다.

Source: http://cafe.naver.com/k2bclub/201


Tactic is
Much more important!

We should also consider when our first tactic fails

Plan B

From Wikipedia, the free encyclopedia

Plan B is a popular term used to mean a reserved, secondary plan, in case a first plan (a hypothetical 'Plan A') fails.


RETURN
TO WORK

I made a formula

Possibility to get Attack =
$\{Value(Money, Shock, Show, Power,\ldots)\}^3$
X Chance X Difficulty

Consumerization
(Java, Windows,
MS Office, acrobat,
hwp, IE, …)

One-Day
Zero-Day
Unknown
…


Java Setup - Progress
Java
ORACLE
CVE-2013-0422 - National Vulnerability Database
web.nvd.nist.gov/view/vuln/detail?vulnId=CVE...
2013. 1. 10. - CVE-2013-0422 covers both the JMX/MBean and Reflection API issues. ...
and JRE 6, 5.0 and 1.4.2, and Java SE Embedded JRE releases are ...
CVE-2013-1487 - National Vulnerability Database
web.nvd.nist.gov/view/vuln/detail?vulnId=CVE...
Vulnerability Summary for CVE-2013-1487. Original release date:02/20/2013 ... line trunk,
spacer, Nav control image, * cpe:/a:oracle:jre:1.7.0:update1 ...
ORACLE

It is time to stack layers

How to stack layers - 1

Different colors

How to stack layers - 2

Different Orders

Filters of the water purifier

1차 세디멘트필터 전처리 정전필터는 녹이나 흙, 모래, 먼지등 비롯한 찌꺼기 등 5미크론의 미세한 불순물까지 제거함으로써 초기단계에서부터 정수효과를 극대화하였습니다.

2차 프리카본필터 활성탄의 흡착방식을 이용한 프리카본필터는 유기화합물질과 냄새등 흡착제거하여 자연에 가까운 물을 만들어줍니다.

3차 UF중공사막필터 0.1~0.4미크론의 미세한 중공사막필터가 물속에 남아있는 불순물을 깨끗하게 걸러내고 미네랄성분이 그대로 함유된 물만을 통과시킵니다.

3차 CSM UF골드필터 중공사막에 비해 저거능력이 10배이상 뛰어나며, 냄새나 맛에 의한 클레임 해소 0.001cm미만의 균일한 필터가 분포되어 저거능력이 우수합니다.

4차 포스트카본필터 물에 스며든 불쾌한 냄새, 맛, 색소성분등을 제거하여 무색, 무취의 깨끗한 물을 만드는 기능을 가진 필터입니다.

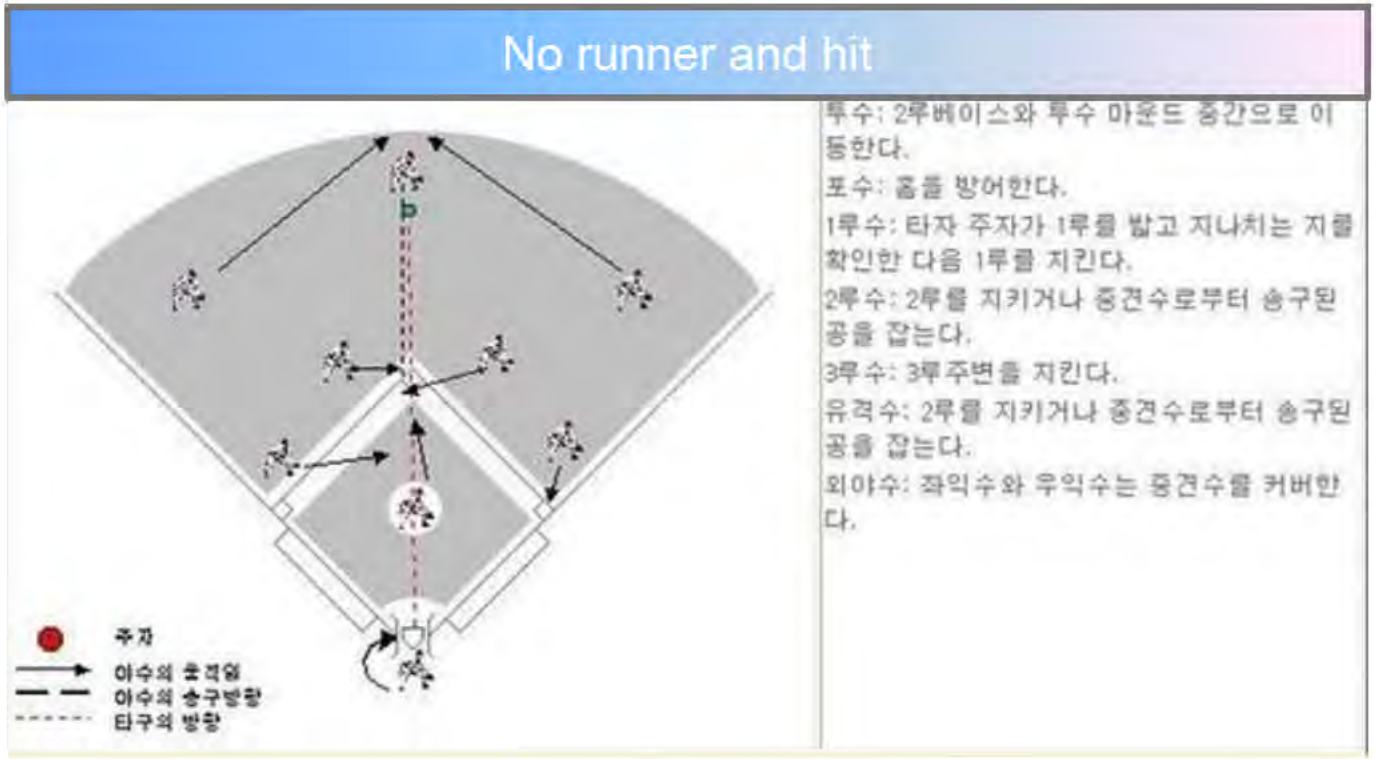
5차 TCR필터 포스트카본용 활성탄에 은(Ag)으로 코팅하여 인체에 유익한 은성분을 첨가함으로써 물의 맛과 카본필터의 성능을 향상시킨 필터입니다.

How to stack layers - 3

Back to the basic
Confidentiality Integrity Availability

But layering is not enough

Baseball



Can't find this kind movement in Cyber security Field

Example 1

My first try in 2005

Easily by-passed

Anti-Keylogger

Can't be sure this is user's input or auto-input

Secure Channel

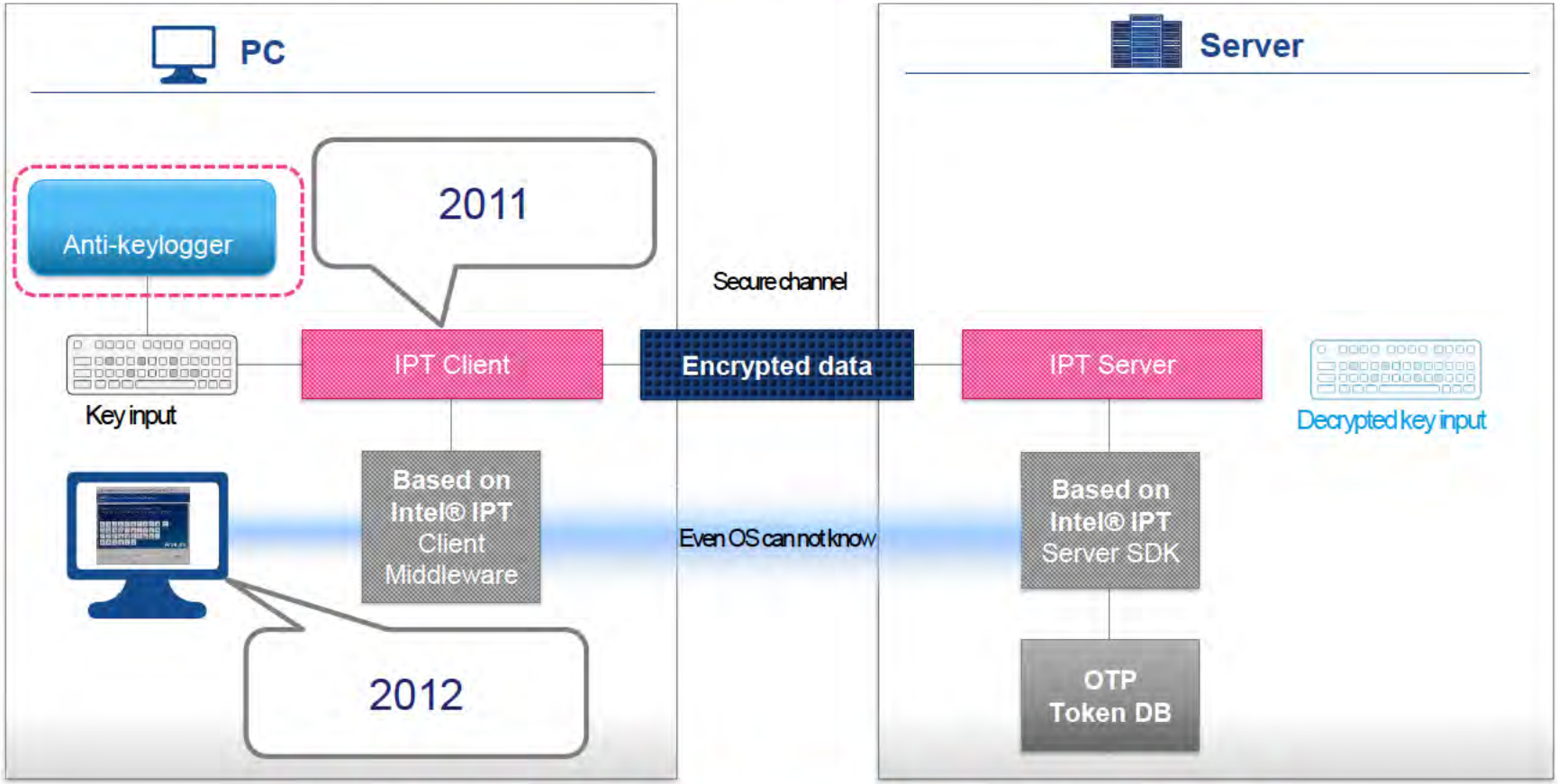
+

ANTI-KEYLOGGER E2E

Hard to by-pass, only passes user input, and protect key logging and eve's dropping

Example 2

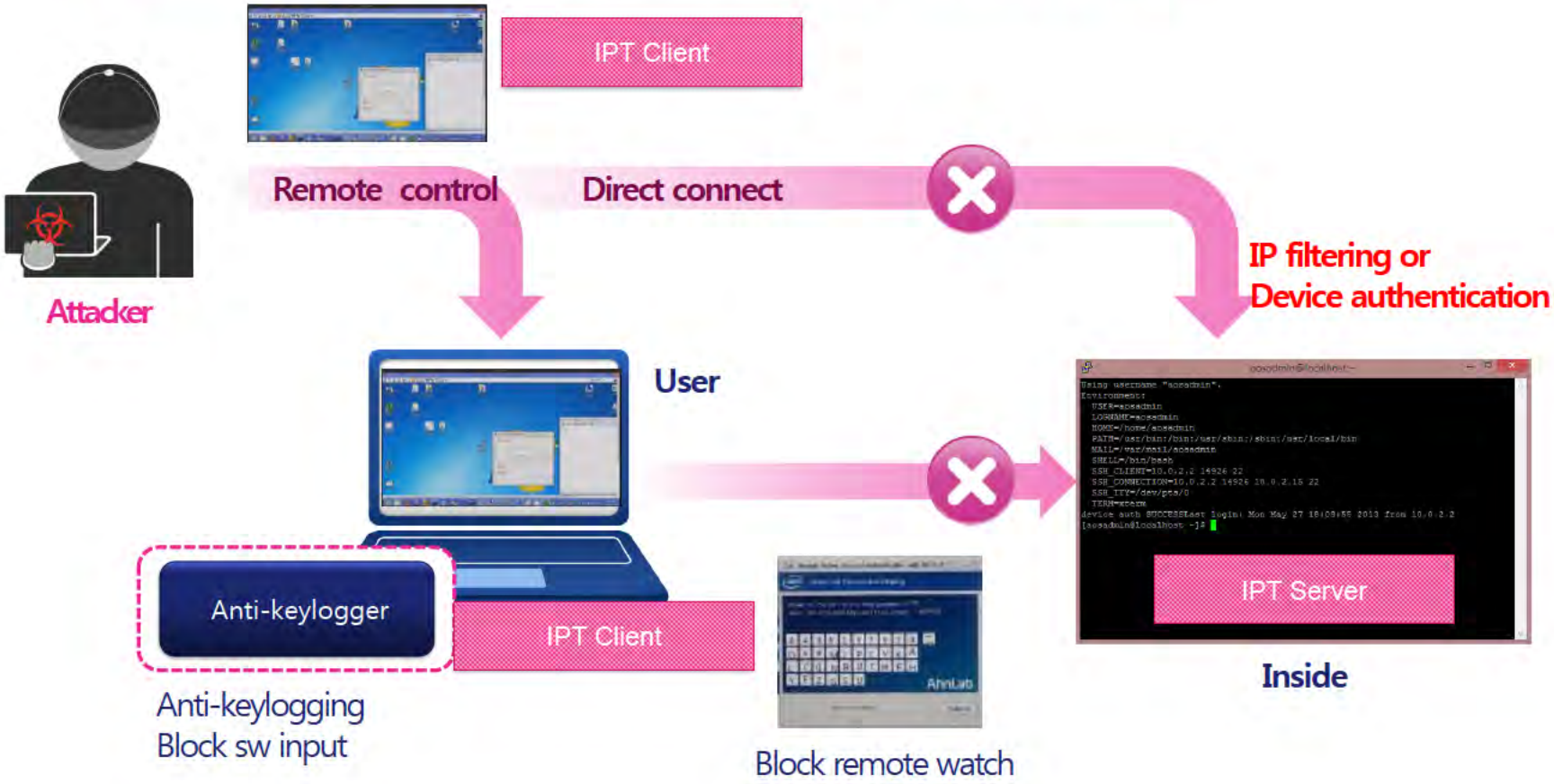
My second try in 2011



SUPPORTED BY HW

Example 2

1. Attacker acquired our id/pwd
2. Attacker can control our pc from remote location
3. Anti-keylogger can be by-passed
4. Blocking of remote watch can last more than 3~4 years. (I hope…)



Example 3

Not My try

Bit9 Launches Endpoint Security Integration with Palo Alto Networks and FireEye

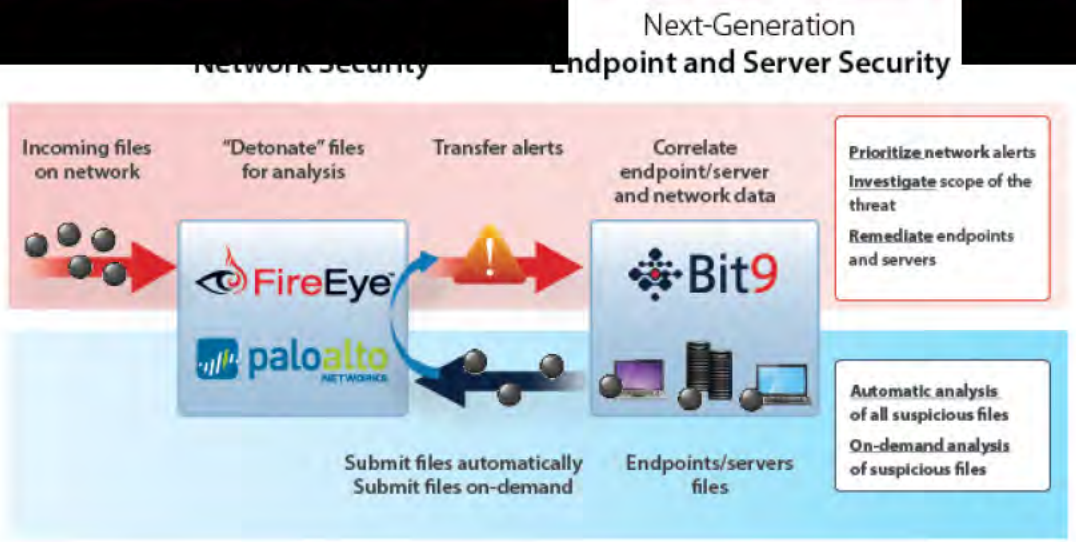
How can you multiply the value of your investment in next-gen security solutions such as FireEye and Palo Alto Networks? With Bit9 Connector.

The Bit9 Connector for Network Security Devices delivers a unique integration of next-gen network and endpoint security platforms that protects organizations from today's advanced cyber-attacks.

How?

When a network device such as FireEye or Palo Alto Networks' detects a suspicious file on the network, Bit9 consumes the alert and automatically confirms the location, scope and severity of the threat on your endpoints and servers.

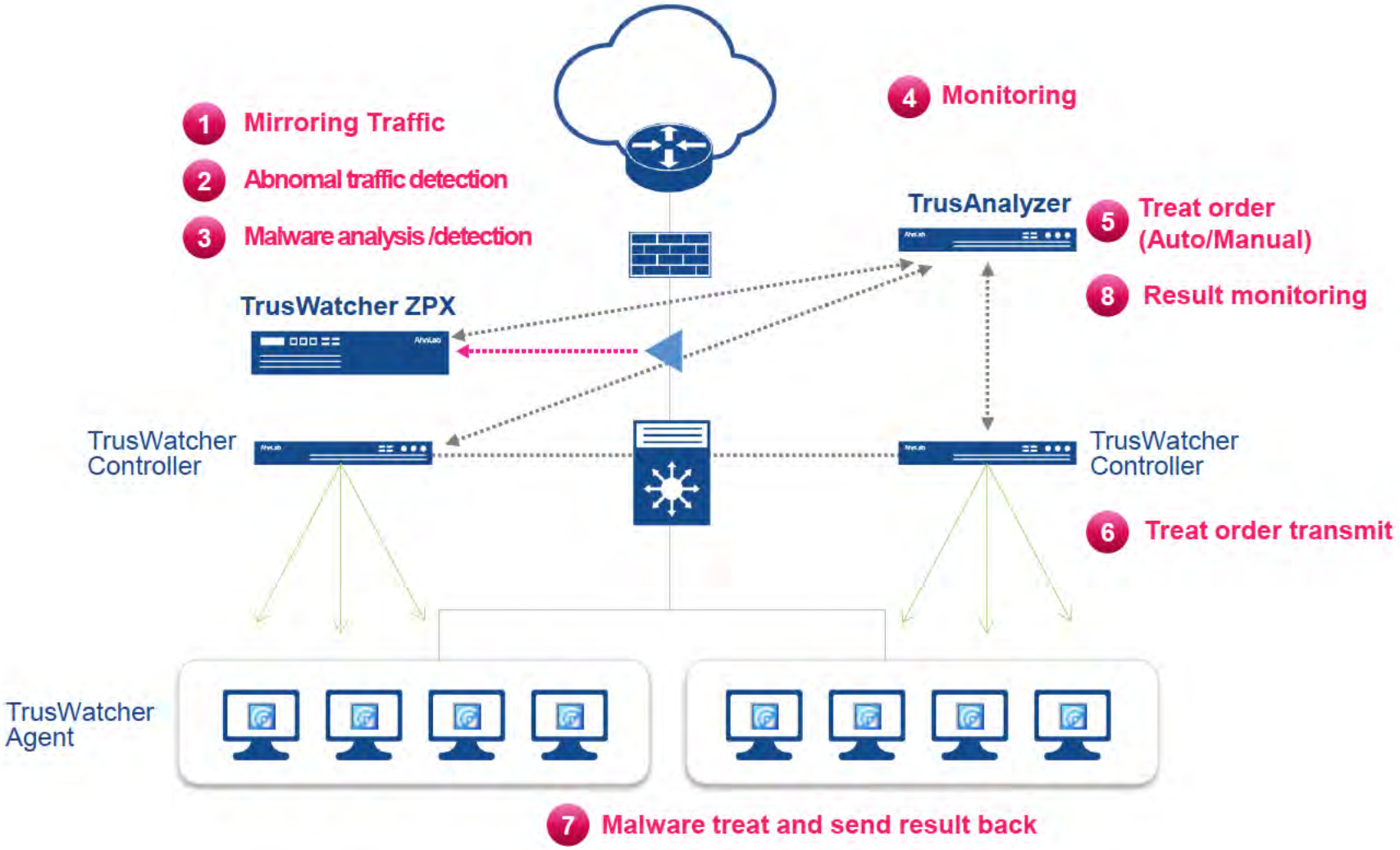
SOME ALREADY STARTED TO ACT



Reduce the time it takes to prioritize alerts and investigate incidents from days to minutes

Example 4

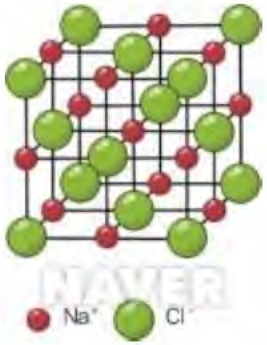
AhnLab's try



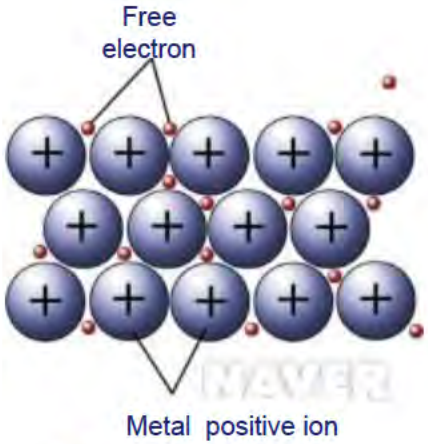
Lesson from Chemistry

From the view of mass

<



<



Covalent bond

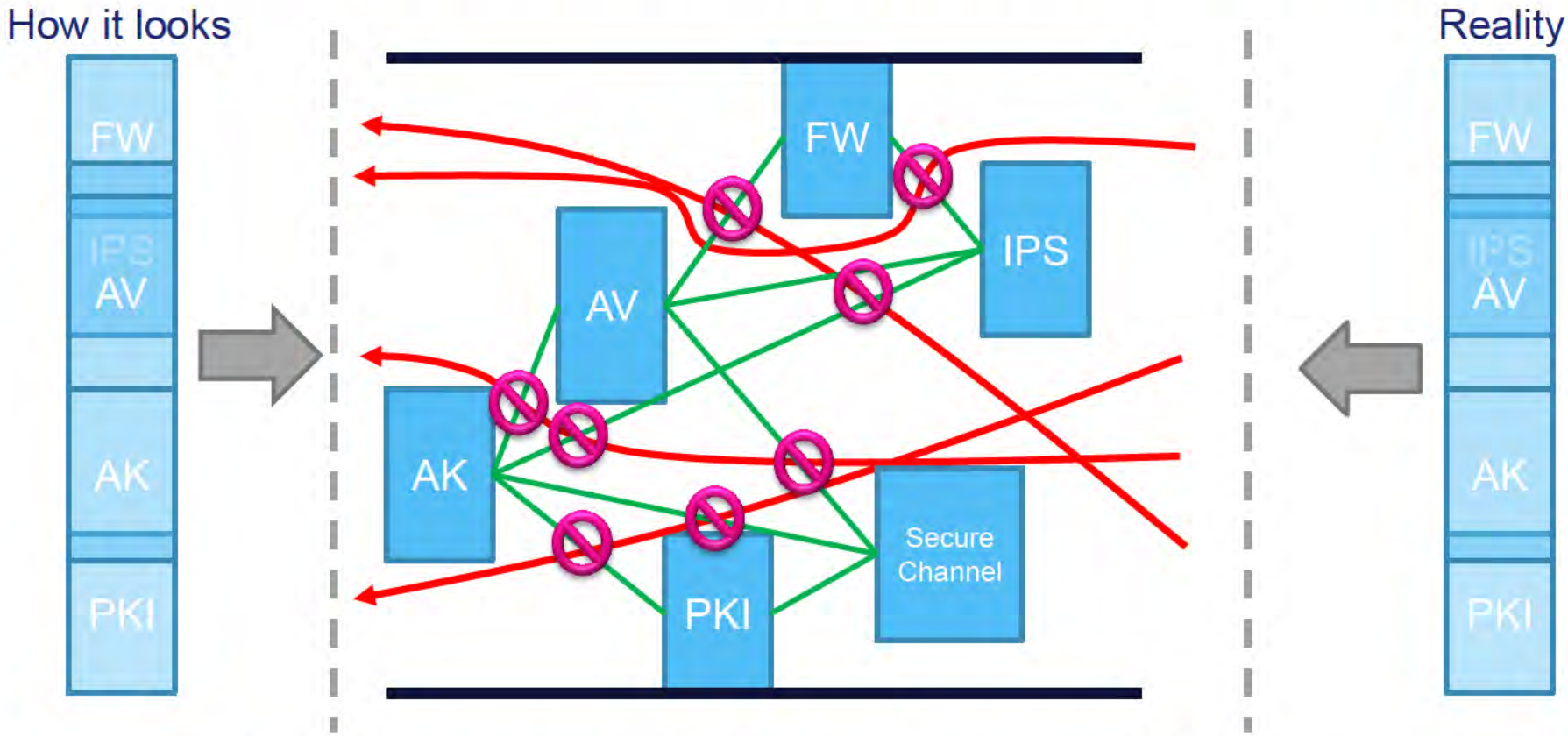
Ion bond

Metal bond

I'M HERE

Solutions can not move but

Information can move like free electron



Then we can close the gap!

Security Technology ≠ Security Product
Security Product ≠ Security