THE PLIGHT OF THE TARGETED ATTACKER IN A WORLD OF SCALE

Cormac Herley
Microsoft Research

CLASSIC ATTACKER MODEL

- Alice must protect her resources from attacker Charles
- Alice's strategy is known to Charles, who adapts
- Alice's security is only as strong as the weakest link
- Alice must guard against every possible attack
- **Alice must have unlimited budget**

HOPELESS

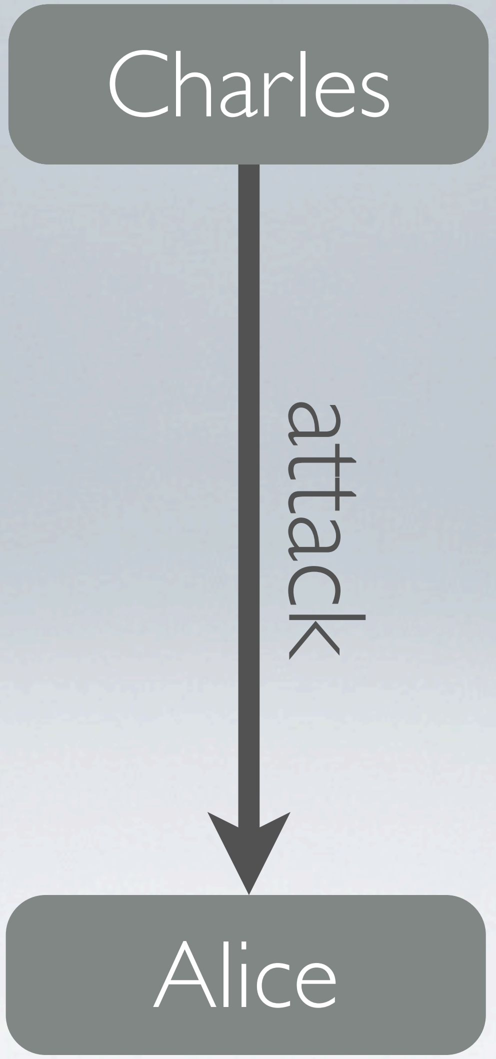
Failure to do everything means there is no point in doing anything.

HOPELESS ?

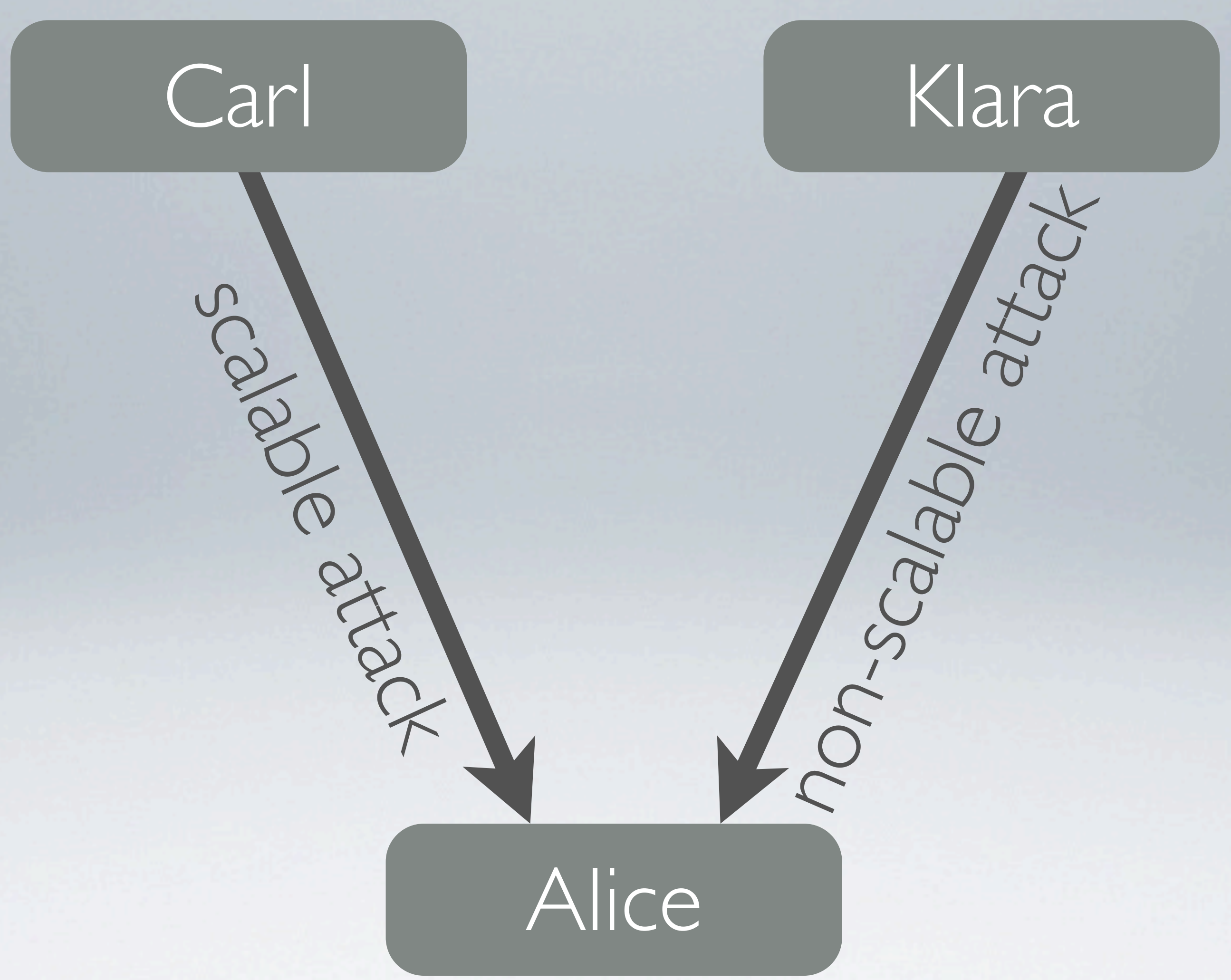
Failure to do everything means there is no point in doing anything.

Most users never experience most attacks.

NEW ATTACKER MODEL



NEW ATTACKER MODEL



Carl

Klara

scalable attack

non-scalable attack

Alice

METRICS

Cost	C	resources invested by the attacker
Reward	R	$R(N) = NY\bar{V}$
Profit	P	$P(N) = R(N) - C(N)$

ATTACK TYPES

	Scalable	Non-scalable
Cost	$C_s(2N) < 2C_s(N)$	$C_n(2N) = 2C_n(N)$
Reward	$R_s(2N) = 2R_s(N)$	$R_n(2N) = 2R_n(N)$
Profit	$P_s(2N) > 2P_s(N)$	$P_n(2N) = 2P_n(N)$

EXAMPLE

- documented spam campaign
- **350 million** emails sent, $2800 reward
- if we assume break-even: $C_s(350 \times 10^6) = \$2800$
- Klara invests 1 hour of minimum wage effort per attack
- she reaches **386** users for the same cost

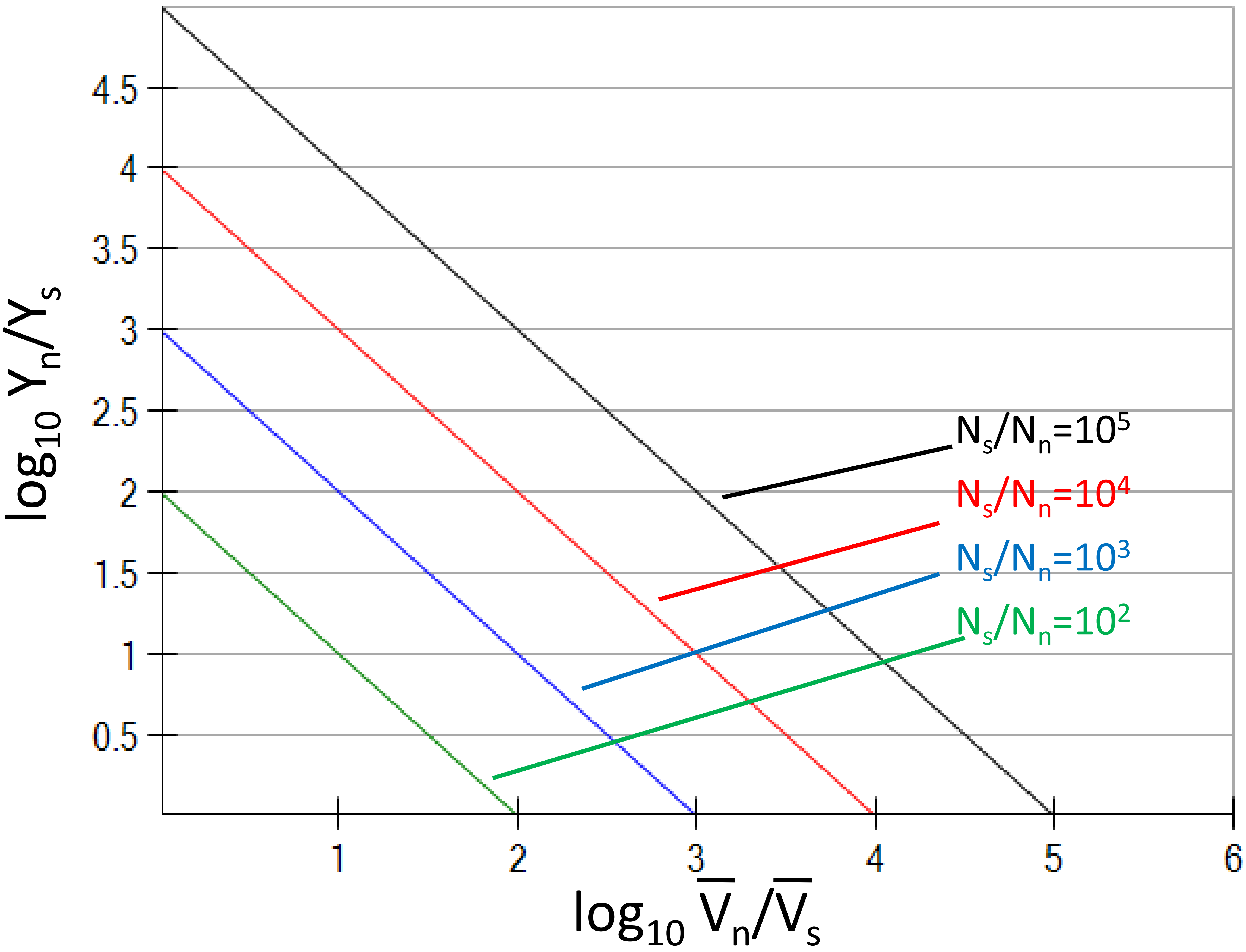
PERSONALIZATION

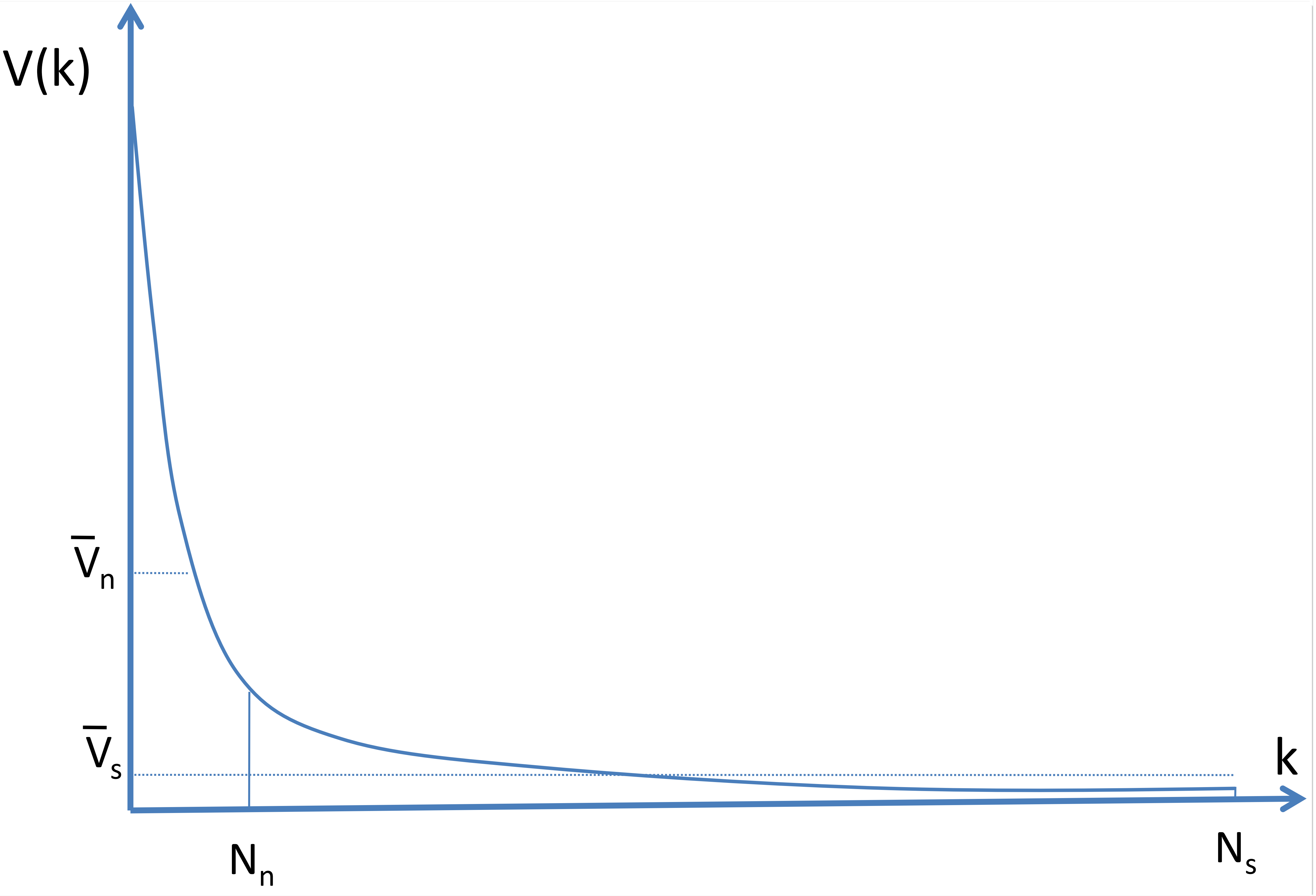
- profitable campaign: $C_s(N) < N_s Y_s \overline{V}_s$
- personalization increases cost and yield
- $C_s'(N) - C_s(N) < (Y_s' - Y_s) \cdot \overline{V}_s$
- targeting may increase yield by 4.5
- cost increase must remain below $0.00002
- **scalable attacks must be entirely automated**

CONSEQUENCES

- scalable attacks cause greater supply of botnets, passwords, …
- value decreases due to mass production

- non-scalable attacker reaches far less victims (N_s / N_n)
- to achieve the same reward ($NY\overline{V}$), Klara must compensate


$\log_{10} Y_n/Y_s$
4.5
4
3.5
3
2.5
2
1.5
1
0.5
1
2
3
4
5
6
$\log_{10} \overline{V}_n/\overline{V}_s$
$N_s/N_n=10^5$
$N_s/N_n=10^4$
$N_s/N_n=10^3$
$N_s/N_n=10^2$


V(k)
$\bar{V}_n$
$\bar{V}_s$
k
N_n
N_s

HIGH-VALUE TARGET

Klara needs longtail distributions.

- concentration of extractable value
- visibility of extractable value

LONGTAIL DISTRIBUTIONS

- 1.8% of US inhabitants exceed average wealth
- literature: half the attention concentrates on 2% of poets
- in a discipline with N scientists, half of the papers are produced by $\sqrt{N}$ of them
- **most users are not profitable targets for non-scalable attacks**

CONCLUSION

Alice's avoidance of harm is not determined by her security measures, but by the worthlessness of the average facebook page.

DISCUSSION

- the paper is obvious: security is not binary, but a **tradeoff**
- who is the victim of targeted attacks: Bill Gates? Sarah Palin?
- what are typical targeted attacks: spearphishing, WEM
- can non-scalable attacks be turned into scalable ones? (think of CAPTCHA-porn)