ISSN 1879-9523
journal of chain-computerisation
information exchange for chain co-operation
Universiteit Utrecht

Professional article

Chains and identity

J.H.A.M. Grijpink

Journal of Chain-computerisation
Information Exchange for Chain Co-operation

2012 – Volume 3, Art. #7

Received: 8 November 2012
Accepted: 1 December 2012
Published: 19 December 2012

2012 – Volume 3, Art. #7
URN:NBN:NL:UI:10-1-113980
ISSN: 1879-9523
URL: http://jcc.library.uu.nl/
Publisher: Igitur publishing, in co-operation with the Department of Information and Computing Sciences, Utrecht University

Copyright: this work is licensed under a Creative Commons Attribution 3.0 Licence

Chains and identity

J.H.A.M. (Jan) Grijpink
Utrecht University, The Netherlands
grijpink.jham@gmail.com

Abstract: Guidelines are presented to cope with identity problems in chains. A chain is a collaboration of a great number of autonomous organisations and professionals to tackle a dominant chain problem. In many chains identity fraud is an aspect of the dominant chain problem. Identity fraud is using some-body else's identity with malicious intent to acquire goods or rights that one is not entitled to. Traces inherently point to the victim, the culprit remaining hidden behind the misused identity. Therefore, only prevention can effectively reduce identity fraud by deterring a fraudster or getting him caught red-handed. Prevention in a chain process can be achieved by simultaneous multifactor identity verifications (token, PIN, transaction code, etc.), because an identity fraudster is unable to manipulate them all consistently at the same time. Multifactor identity verification in a closed interactive communication loop also produces meta-data (for example, the result of a calculation or a telephone number) that can be used for consistency checking, as well.

Keywords: identity, identity fraud, chain, ID protocol, multifactor identity verification, interactive communication loop

---

1 Outline

1. Many chains are confronted with a dominant chain problem with an identity fraud/identity theft component. The dominant chain problem determines how unambiguous a designation or recognition of a person or object should be.
2. Identity fraud – with malicious intent deliberately evoking the appearance of an identity that does not belong to you – can be done anywhere and in many different ways. If an identity fraud has been successful by a weakness in a particular chain, that wrong identity can spread unnoticed to other chains. The consequences depend on the situation in which the identity fraud/theft did occur.
3. If an identity fraud succeeds, the traces point to the victim, the perpetrator often remaining invisible and untraceable. Therefore, only prevention is effective.
4. The digitisation of our society is boosting identity fraud/identity theft in at least three new dimensions increasing its impact and frustrating fighting it: more traces, less evidence; snowball effect of identity fraud/identity theft; a power shift in a digital environment.

2 Explanation

Chains are temporary patterns of cooperation between large numbers of more or less autonomous organisations and professionals, enforced by a dominant chain problem. Because large-scale systems behave differently than small-scale systems such as an organisation, we often make so-called mistakes of the wrong level which

in system and information management give rise to wrong assumptions and unrealistic expectations.

Where we speak of identity we mean the social identity, some formal characteristics with which we designate or recognise a person or object. Many chains are confronted with a dominant chain problem with an identity fraud/identity theft component. The dominant chain problem determines how unambiguous a designation or recognition of a person or object should be.

In uncontrollable chain processes, more attention is needed for identity fraud/identity theft, here defined as deliberately and with malicious intent evoking the appearance of an identity that does not belong to you. Depending on the dominant chain problem this can compromise and disrupt the chain as a whole. In the criminal justice system identity fraud (alias abuse) has been frustrating criminal law enforcement (wrong culprit, wrong punishment) leading to severe pollution of the criminal registry causing detention or arrest of wrong people. In medical treatment ID fraud causes medical data of somebody else to be recorded in the file of the official holder of an e-health number (BSN), sometimes with serious consequences.

Piggyback on another identity is usually not difficult, provides many advantages if successful and virtually no downside if not. The digitisation of our society is boosting identity fraud/identity theft in at least three new dimensions increasing its impact and frustrating fighting it:

More traces, less evidence. A successful identity fraud inherently leaves traces pointing to the victim, the perpetrator often remaining untraceable. Therefore, only prevention is effective, but many procedures have little or no preventive components.

Snowball effect of identity fraud/identity theft. Successful identity fraud spreads like wildfire into the smallest administrative capillaries of various social processes where the primary identity fraud often cannot be seen nor understood.

Power shift in a digital environment. Traditionally, the inspector is in charge, the person being checked should respond. In digital procedures – or when using digital equipment – the person being checked is the boss. He is able to provoke an emergency procedure unnoticed, e.g. with a damaged chip. It is the inspector who then has to improvise and act on what is being told or shown.

Only prevention can reduce identity theft/identity fraud by deterring a fraudster or getting him caught red-handed. This is mainly achieved by the simultaneous use of multiple verification tools (PIN, transaction code, etc.), because an identity fraudster is unable to manipulate them all consistently at the same time. If you apply 'three or four times knocking' in a closed interactive communication loop, you can use any return data (for example, the result of a calculation or telephone number) for consistency testing, as well.

3 Guidelines

1. When developing or managing large-scale systems, build your plans and projections on the premise of massive use and barely-controllable conditions. Find unexpected risks before they find you.
2. Develop chain-specific ID protocols and test them on robustness against identity fraud.

3. Provide variety and surprises in ID procedures to make identity fraudsters uncertain of success. That scares them off.
4. Organize closed, interactive communication loops that are resistant to identity fraud. Make simultaneously use of multiple instruments: "three or four times knocking".
5. Use independent data. Information presented by the person being checked is not usable (anymore) for control.

Biographical notes: Professor Jan Grijpink (1946) is Emeritus Professor of Information Science at Utrecht University where he part time lectured in Chain-computerisation. He studied Economics (1969) and Law (1971) at Groningen University. In 1997 he obtained his doctorate at Eindhoven Technical University with a thesis about Chain-computerisation.

As Principal Adviser at the Dutch Ministry of Justice until his retirement in 2011, he focused on information strategy and identity issues. He is Senior Adviser of PLBQ/The Center of Expertise, IT consultants of the Dutch government. He is the initiator and coordinator of the Platform Chain-computerisation and editor of the Journal of Chain-computerisation. He is editor-in-chief of the open access Journal of Chain-computerisation.
Jan Grijpink regularly publishes on identity issues in a complex information society often using his professional focus on large-scale information systems and chain-interdependencies to uncover hidden problems or develop better solutions.

References

Grijpink, J. H. A. M. (2008). Checklist Identiteitsfraude [Checklist Identity Fraud]. *Checklisten Informatiemanagement, 2008-2, 1.B.7*. Den Haag: Sdu Uitgevers.

Grijpink, J. H. A. M. (2006a). Criminal Records in the European Union, the challenge of large-scale information exchange. *European Journal of Crime, Criminal Law and Criminal Justice*, *14*(1), 1-19. Leiden: Brill Academic Publishers.

Grijpink, J. H. A. M. (2006b). Identiteitsfraude en overheid [Identity fraud and government]. *Justitiële Verkenningen*, *7*(6), 37-57. Den Haag: WODC/Boom Juridische Uitgevers.

Grijpink, J. H. A. M. & Plomp, M. G. A. (red.) (2009), *Kijk op ketens. Het ketenlandschap van Nederland [Focus on chains. The chain landscape of the Netherlands]*. Den Haag: Centrum voor Keteninformatisering BV.

Grijpink, J. H. A. M. (2011a). Public Information Infrastructures and Identity Fraud. In S. van der Hof & M. Groothuis (red.), *Innovating Government. Normative, Policy and Technological Dimensions of Modern Government*, pp. 363-381. The Hague: TMC Asser Press/Springer Verlag.

Grijpink, J. H. A. M. & Plomp, M. G. A. (2011b). Combating Identity Fraud in the Public Domain: Information Strategies for Healthcare and Criminal Justice. Proceedings of the 11th European Conference on E-Government (pp. 451-458). Reading UK: Academic Publishing Ltd.

Grijpink, J. H. A. M. (2012). Large-scale Information Exchange: Breaking Views and Challenges. In I. Snellen, M. Thaens & W. Van de Donk (red.), *Public Administration in the Information Age: Revisited,* pp. 182-204.